UNITED STATES MARINE CORPS
MARINE CORPS SYSTEMS COMMAND
2200 LESTER STREET
QUANTICO, VIRGINIA 22134-5010

IN REPLY REFER TO:
5720
DON-USMC-2018-002851
18 Jan 18

EMAILED TO: foia@foia.com

Ms. Rose Santos
FOIA Group
P.O. Box 368
Depew NY 14043

SUBJECT: DON-USMC-2018-002851

Dear Ms. Santos:

This letter responds to your Freedom of Information Act request dated January 4, 2018, requesting a copy of the title page and the Performance Work Statement associated with contract M67854-17-F-4419.

The requested documents are enclosed.

As of January 18, 2018, one hour of search and review (currently billed at $48 per hour) has been expended during the processing of your request. Please remit a check or money order, payable to the Treasurer of the United States in the amount of $48.00 to: COMMANDER, ATTN LAW, MARCORSYSCOM, 2200 LESTER STREET, SUITE 120, QUANTICO VA 22134-5010.

If at any time you are not satisfied that a diligent effort was made to process your request, you may file an administrative appeal with the Assistant to the General Counsel (FOIA) at:

Department of the Navy
Office of the General Counsel
ATTN: FOIA Appeals Office
1000 Navy Pentagon Room 4E635
Washington DC 20350-1000

Any questions concerning this matter should be directed to Mrs. Bobbie Cave at (703) 432-3934 or bobbie.cave@usmc.mil.

Sincerely,

Bobbie Cave

for Lisa L. Baker
Counsel

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30

1. REQUISITION NUMBER	PAGE 1 OF 62
SEE SCHEDULE	

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
GS00Q09BGD0015	25-Sep-2017	M6785417F4419	M67854-17-R-4419	

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No Collect Calls)*	8. OFFER DUE DATE/LOCAL TIME
	DEBORAH PICKERAL	703-432-7490	

9. ISSUED BY CODE M67854

COMMANDER, MARINE CORPS SYSTEMS COMMAND
ATTN: TARASIA REMHOF
2200 LESTER STREET
QUANTICO VA 22134

TEL: 703-784-6555
FAX: 703-784-6829

10. THIS ACQUISITION IS

[X] UNRESTRICTED OR [ ] SET ASIDE: _____ % FOR:

[ ] SMALL BUSINESS
[ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
[ ] HUBZONE SMALL BUSINESS
[ ] EDWOSB
NAICS: 541519
[ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
[ ] 8(A)
SIZE STANDARD: $27,500,000

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
[ ] SEE SCHEDULE	Net 30 days	[ ]	[ ] RFQ [ ] IFB [X] RFP

15. DELIVER TO CODE M67854

COMMANDER MARCORSYSCOM
REGINA WASHINGTON
2200 LESTER ST.
QUANTICO VA 22134

16. ADMINISTERED BY CODE

SEE ITEM 9

17a. CONTRACTOR/ OFFEROR CODE 7N699 FACILITY CODE

AT&T GOVERNMENT SOLUTIONS, INC.
LISA SINGLETARY
1900 GALLOWS RD STE 105
VIENNA VA 22182-3865

TELEPHONE NO. 703-439-9267

18a. PAYMENT WILL BE MADE BY CODE M67443

DFAS COLUMBUS
DEFENSE FINANCE & ACCOUNTING SERVICE COLUMBUS
DFAS-JDCBB/CO
PO BOX 182317
COLUMBUS OH 43218-2317

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED [X] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	SEE SCHEDULE				

25. ACCOUNTING AND APPROPRIATION DATA

See Schedule

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

$6,732,525.74

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

[ ] 29. AWARD OF CONTRACT: REF. OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

Tarasia L. Remhof

30b. NAME AND TITLE OF SIGNER *(TYPE OR PRINT)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(TYPE OR PRINT)*	31c. DATE SIGNED
		Tarasia L. Remhof / Contracting Officer TEL: 703-432-9893 EMAIL: tarasia.remhof@usmc.mil	22-Sep-2017

PERFORMANCE WORK STATEMENT (PWS)

FOR THE

Information Technology Service Management (ITSM) – Marine Corps

Operations and Sustainment (O&S)

January 25, 2017

Prepared for:

PdM Marine Corps Network and Infrastructure Services

Information Systems & Infrastructure

Marine Corps Systems Command

Quantico, Virginia 22134

Table of Contents

1.0 General 4
1.1 Description of Services/Introduction 4
1.2 Background 4
1.2.1 ITSM Program History 4
1.2.2 ITSM Tool Suite 6
1.2.3 Systems Engineering Approach 7
1.2.4 Anticipated State at Task Order Award 7
1.3 Scope 9
1.4 General Information 10
1.4.1 Place of Performance 10
1.4.2 Post Award Conference/Periodic Progress Meetings 10
1.4.3 Travel and Other Direct Costs (ODCs) 11
1.4.4 Period of Performance (PoP) 11
1.4.5 Adherence to Marine Corps Documentation 11
1.4.6 Documentation Requirements 12
1.4.7 Coordination with Concurrent Efforts 13
1.4.8 Process Adherence 14
1.4.9 SME Skill Set Requirements 14
1.4.10 Personnel Access Requirements 18
1.4.11 Code Review 19
1.4.12 Implement, Monitor and Report on Contract Risks 19
2.0 Performance Requirements 19
2.1 Objectives 19
2.1.1 Objective 1: Program Management 19
2.1.2 Objective 2: ITSM Tool Suite Operations and Maintenance 25
2.1.3 Objective 3: Enhancement of ITSM Training Materials 48
2.1.4 Objective 4: ITSM Toolset Training Environment 50
2.1.5 Objective 5: ITSM Toolset Configuration and Enhancement Environment 51
2.1.6 Optional Objective 6: ITSM Tool Suite Enhancement 53
2.1.7 Optional Objective 7: ITSM Training Activities 56
3.0 Government Furnished Equipment (GFE) and Government Furnished Information (GFI) 58
3.1 Information 58
3.2 Government-Furnished Property/Equipment (GFP/GFE) 59

4.0 Contractor Furnished Items and Responsibilities 59
4.1 General 59
4.2 Security Requirements 60
4.3 Common Access Card (CAC) Requirement 62
4.4 Certification and Accreditation (C&A) 63
4.5 ITSM tools Configuration, Enhancement and Testing Environments 63
5.0 Definitions 63
5.1 Deliverables 63
5.2 Contracting Officer (KO) 63
5.3 Contracting Officer's Representative (COR) 63
5.4 Quality Assurance (QA) 63
5.5 Quality Assurance Program Plan (QAPP) 64
5.6 Quality Control (QC) 64
6.0 Applicable Publications (Current Editions) 64
6.1 Compliance Documents 64
6.2 Security Related Guidance 64
6.3 Standards 65
6.4 Other Guidance 66
7.0 Acronyms 66
Appendix A - Performance Requirements Summary..... 73
Appendix B –Program Deliverables..... 85

PERFORMANCE WORK STATEMENT (PWS)

Information Technology Service Management (ITSM) – Marine Corps

1.0 General

The purpose of this document is to provide a Performance Work Statement (PWS) for the Marine Corps ITSM Operations and Sustainment (O&S) of ITSM supporting tools and technologies.

1.1 Description of Services/Introduction

The Contractor shall provide ITSM O&S for the United States Marine Corps (USMC) as defined in this PWS.

1.2 Background

The Marine Corps Garrison networks have recently undergone a transition from a Contractor-owned, Contractor-operated (COCO) to a Government-owned, Government-operated (GOGO) environment. In support of this transition the Marine Corps has established a comprehensive, integrated ITSM implementation based on Information Technology Infrastructure Library (ITIL) Version 3. This solution implements industry best practices while conforming to Department of Defense (DoD), Department of Navy (DON), and Marine Corps standards, policies, and guidance.

The Marine Corps' vision, strategy, and planning documents, intended to unify and synchronize the efforts of the Marine Corps IT community, are the Marine Corps Information Enterprise (MCIENT) Strategy and the Marine Corps Information Environment (MCIE) Supporting Establishment (SE) Concept of Employment (COE) and Marine Corps Enterprise Network (MCEN) Unification Plan.

1.2.1 ITSM Program History

The ITSM program captures and documents IT management processes and tools for the Marine Corps classified and unclassified garrison IT environments to include processes, architectures, roles, and responsibilities. The Marine Corps ITSM implementation includes the following ITSM processes at varying levels of maturity:

- Service Catalog Management (SCM)
- Incident Management (IM)
- Change Management (ChM)
- Release & Deployment Management (RDM)
- Event Management (EM)
- Service Asset & Configuration Management (SACM)
- Request Fulfillment (RqF)

- Problem Management (PbM)
- Knowledge Management (KM)
- Identity and Access Management (IdAM)
- Demand Management (DM)
- Capacity Management (CpM)
- Availability Management (AvM)
- Service Level Management (SLM)

BMC Remedy is the service management platform used for tracking and managing USMC IT processes, activities, and assets. Remedy enables multiple process areas to manage data specific to their process while allowing each process to seamlessly share and relate information and activities through record association. The capability of the Remedy tool provides for the creation and storage of various types of records, including incident records, problem records, change records, release records, request records, asset records, contracts and warranties records, and software license records. BMC Remedy provides reporting and dash-boarding capabilities for all system records, attributes and data elements. Remedy also houses a searchable repository of knowledge articles that can be associated with designated system modules, workflows, and custom applications.

The Marine Corps has also implemented the Hewlett Packard (HP) operations management tool suite across the Marine Corps using a hub and spoke model utilizing "regional aggregators" (located across the globe) to perform network operations and configuration management functions at regional locations. This model allows regional users to fully manage their component of the overall network while at the same time sending network event information to a centralized monitoring system at the Marine Corps Enterprise Information Technology Services (MCEITS) in Kansas City, MO. This capability allows Marine Corps operations to have a seamless view of the entire Marine Corps Enterprise Network (MCEN) supporting network operations and defense while enabling timely threat management and problem resolution.

In support of USMC Service Asset and Configuration Management (SACM), the Marine Corps established an enterprise Configuration Management Database (CMDB) utilizing BMC Atrium. The USMC CMDB was built to store all USMC Configuration Items (CI) and to provide a clear picture of enterprise physical and virtual assets including

their relationship to each other. The Marine Corps implemented a custom BMC Remedy Tech Refresh workflow automation within the Asset Management console that allowed regional Asset Managers the "enhanced" ability to plan and execute major non-data center asset refreshes across the enterprise.

In addition to the Tech Refresh workflow, the Marine Corps also established limited IT license management automation for software licenses located with the MCNIS portfolio. This provides tracking of software license compliance in Remedy using the contracts, asset inventory data, and network-discovered data of desktops and laptops stored in the CMDB.

As part of providing IT "Services" for the USMC, the Marine Corps has established an enterprise service catalog comprising of orderable and technical enterprise services. USMC has integrated the Service Request Module (SRM) with Incident Management, Work Order Management, and Change Management allowing users requesting services to have a fully transparent view from ordering through fulfillment.

The Marine Corps has also developed and delivered Computer-Based Training (CBTs), Job Aids, and Just-in-Time videos in order to explain ITSM processes and their supporting toolsets. These CBTs and Just-in-Time videos ensure that the operator and the Warfighter have adequate ITSM training.

1.2.2 **ITSM Tool Suite**

The ITSM tool suite that supports Marine Corps ITSM processes includes but is not limited to the following (upgrades are ongoing and version numbers may change):

- BMC Remedy Suite 8.1.0.2
- Hewlett Packard (HP) Operations Management Tool Suite 9.x
- Oracle 11.x
- RedHat Linux
- Microsoft (MS) Windows 2008
- MS SQL Server 2012
- VMware vSphere

A detailed list of tools and the infrastructure supporting them is provided as Government Furnished Information (GFI) in Section 3.0 of this document.

1.2.3 **Systems Engineering Approach**

ITSM systems are designed and acquired according to the system engineering acquisition approach described in DoDI 5000.02, Secretary of the Navy Instruction (SECNAVINST) 5000.2D, and the Defense Acquisition Guidebook.

In addition, these systems must be implemented in accordance with the Systems Engineering Technical Review (SETR) process as stated in the MARCORSYSCOM Technical Review Handbook v1.04(MARCORSYSCOM Order 4130.1).

1.2.4 **Anticipated State at Task Order Award**

1.2.4.1 Current State

The current state of ITSM tools is explained below.

The ITSM toolset suite is installed, configured, and customized according to Marine Corps ITSM Technical Data Packages (TDPs) and Marine Corps Enterprise Information Technology Services (MCEITS) technical documentation, provided as GFI.

USMC personnel including the Marine Corps Network Operations and Security Command (MCNOSC), Kansas City EITC, Zone A, Regional Network Operations and Security Centers (RNOSCs), MITSCs, and Base/Post/Stations (B/P/S) have received ITSM training in accordance with existing Marine Corps ITSM Training Documentation including Computer-Based Training (CBT), Job Aids, Just-in-Time videos, and other training documents.

The Marine Corps ITSM Service Catalog is housed in the BMC Remedy Service Request Management (SRM) module and is populated with an orderable set of services related to enterprise hardware and software.

Many Request Fulfillment (RqF) workflows, including Hardware and Software ordering, are implemented within the Remedy Service Request Module, a custom application that receives and manages all orders placed via the USMC Product Ordering service request module. The RqF capability also enables limited automated integration with the Information Technology Procurement Request Review/Approval System (ITPRAS) (service request approval system).

Event Management (EM) tools receive event notifications from several different elements and element managers. The Marine Corps has created some correlation rules and filters.

The Knowledge Management module in Remedy is fully implemented and contains over 5,000 Knowledge articles with

the ability to create, review, and approve new articles and search existing articles. It is fully integrated with the Remedy Service Request, Incident, and Problem Management modules.

Mail Integration has been implemented by providing the Remedy system with a Microsoft Outlook client and domain account to enable outgoing email to users receiving Remedy record assignment. Incoming email replies are received by Remedy and recorded into the work detail fields of the corresponding record.

1.2.4.2 Existing ITSM Toolset Environments:

Several ITSM Toolset environments have been set up.

- uPROD - Production environment that employees and authorized personnel use for day to day work. Also referred to as unclassified EITC (uEITC). Connected to the MCEN-N (NIPR) and also available externally via CAC.
- cPROD - Production environment on the secure network. This is also known as the Classified EITC (cEITC). This requires SIPR access permissions.
- ZONE A - MCEITS hosted environment formerly known as (System Integration Environment) SIE. This is the official test and integration environment for systems that are transitioning into the MCEITS production environments.
- MCTSSA Training Stack - Online copy of production with test data used for validation and training hosted at MCTSSA Camp Pendleton and available on the MCEN-N. This environment is not accessible from USMC legacy networks. This environment includes an offline clone of the MCTSSA Training Stack, which is only accessible to people physically at MCTSSA Camp Pendleton with no network connectivity. The offline clone serves as a test environment for changes to the training stack before applying to the online environment.
- Contractor tools configuration sandbox Environment – A tools configuration enhancement stack hosted by the incumbent contractor at the contractor facility utilizing government property. This environment will be decommissioned as part of current contract

closeout. This tools configuration enhancement environment will be reestablished within the Marine Corps Systems Command (MCSC) lab as defined in Section 2.1.5.

Production ITSM tools in the Unclassified EITC (uEITC), Classified EITC (cEITC), and Zone A are operating under an Authority to Operate (ATO).

The Marine Corps USMC training lab at MCTSSA, Camp Pendleton is accredited and available for training and testing use. This system will be a stand-alone system and is remotely accessible through MCEN.

1.2.4.3 Asset Management

A software asset management capability is partially implemented within the Remedy Software Asset Management module by the creation and management of some contract configuration items.

The USMC ITSM Toolset relies heavily on authoritative data including:

- System Center Configuration Manager (SCCM) polls USMC desktops and laptops for asset information which is used to populate the BMC Atrium CMDB.
- Microsoft Active Directory (AD) is the authoritative source of information for organizational structures and enterprise user accounts. AD user accounts are used to populate ITSM system accounts.

HP Operations Management Tool Suite performs partial discovery of servers and infrastructure items which is to populate the BMC Atrium CMDB.

1.3 Scope

The Contractor shall support Marine Corps ITSM operations, and assist the Government in expanding and sustaining Marine Corps ITSM capabilities across the enterprise. The Contractor's primary role is to enhance the Government's ability to execute ITSM. This scope includes planning, system enhancement, documentation, configuration, systems engineering, operational support, integration, installation, Certification & Accreditation (C&A), training, maintenance and testing. The task also covers implementation and support services for the Government-owned software tools that support these processes.

1.4 General Information

1.4.1 Place of Performance

The primary place of performance for this contract will be in the National Capital Region and Government facilities at the following Marine Corps locations:

- MCNOSC, Quantico, VA
- MCTSSA, Camp Pendleton, CA
- MCSC Lab, Quantico, VA

The government will provide desk space and telephones within these facilities for all Contractors supporting the objectives, as well as required badges and accesses that have been approved.

Tasks involving live operational support and deployment must be conducted at the MCNOSC. Tasks involving design, system configuration/enhancement and testing must be conducted at the MCSC Lab. In order to facilitate innovation within proposed technical approaches, the government will allow up to four (4) tool SMEs supporting design and system enhancement efforts and unclassified support operations to perform support activities from remote Contractor locations. The Government will not provide desk space and telephones for SMEs operating from remote Contractor locations, nor will the Government fund travel for these Contractor employees unless explicitly approved in advance by the Government. The travel approval will be strictly restricted to Government work that requires in person attendance.

1.4.2 Post Award Conference/Periodic Progress Meetings

The Contractor shall attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation (FAR) Subpart 42.5. The Contracting Officer (KO), Contracting Officer Representative (COR), and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the KO will apprise the Contractor of how the Government views the Contractor's performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues.

1.4.3 **Travel and Other Direct Costs (ODCs)**

The Contractor may be required to conduct long distance travel in support of the requirements defined above; all travel will be in accordance with the Federal Acquisition Regulation (FAR), including FAR Part 31, and consistent with the limits in the Federal Travel Regulations (FTR). The number of Contractor personnel required for each trip will be validated and approved by the MCSC ITSM Project Officer before the travel occurs. As stated in FAR Subpart 31.2, per diem costs that exceed the rates in the FTR will be found unreasonable. The Government expects the Contractor's staff to be located within a reasonable commuting distance from the primary installation they are supporting (see 1.4.1 above). The Government will not pay travel costs for Contractor staff to commute to work. Any reimbursable travel incurred during the performance of the contract and its associated TOs shall not include travel for day-to-day work activities. The Government will not reimburse local travel. Local travel is defined as travel within a 50-mile radius of the Contractor's place of performance or designated Government installation. The Travel/Other Direct Costs (ODC) in direct support of the tasks included in this PWS will be reimbursed against non-fee bearing Time and Materials Contract Line Item Number (CLIN).

All Marine Corps printing requirements MUST be done by or through Government Printing Offices (GPO) per FAR 8.8, http://USMC classified network domain.daps.dla.mil/dapsonline.html). Any ODC requests for printing requirements MUST be obtained and approved by the KO ONLY, prior to conducting these services and only after submitting applicable waiver documents to the Marine Corps.

The Travel and ODCs are not to exceed **$169,000 per year**.

1.4.4 **Period of Performance (PoP)**

The PoP shall be for one (1) base period of twelve (12) months from date of contract award and three (3) twelve-month option periods, and in accordance with FAR 52.217-8 Option to Extend Services, a six-month extension period.

1.4.5 **Adherence to Marine Corps Documentation**

The Contractor's efforts shall conform to Government provided Marine Corps ITSM process and tool documentation. This documentation, includes process guides, Technical Data Packages (TDPs), Functionality Definition Documents (FDDs),

Procedures/Work Instructions (P/WIs), training documentation and artifacts, and defines the process environment and detailed tool design that form the Marine Corps ITSM configuration baseline. The Contractor shall recommend updates, based on lessons learned and analysis of Government-approved changes. The Contractor shall update these documents based only on Government-approved changes.

Some of the Marine Corps ITSM tool components reside within the MCEITS EITC and Zone A Infrastructure. When this is the case, the Contractor shall conform to the MCEITS design documentation in all configurations and shall propose changes to MCEITS documentation using the Marine Corps ChM processes and applicable MCEITS procedures.

In addition, the Contractor shall follow DoD, DON, and Marine Corps standards, policies, and guidance for Information Assurance (IA), Network Operations (NetOps), and systems engineering. The Contractor shall also consider industry best practices. Specific requirements and guidance are provided in the GFI section of this document.

All documentation updates must be accepted by the appointed Marine Corps POC and approved by the ITSM Contracting Officer Representative (COR). The Contractor will coordinate and facilitate adjudication meetings to elicit Government acceptance or rejection comments, including those provided by the Government and those provided by the Contractor. The Contractor will ensure that the documentation reflects the live system wherever the Contractor has administrative permissions and an approved request for change (RFC) to make necessary changes. Scope of documentation includes:

- Procedures/Work Instructions (P/WI)
- Functional Design Documents (FDD)
- Technical Data Packages (TDP)
- Testing artifacts
- Training Packages
- Engineering documents
- Other supporting plans

1.4.6 **Documentation Requirements**

The Contractor shall provide all technical deliverables in an editable format to facilitate continual improvement by the Government. The Contractor may compress technical information into formats such as but not limited to bmp, html, pdf, jpeg, or png within primary deliverables, but if

so, shall provide the original, modifiable file for each compressed image or data element. For example, the Government must be able to change the source and destination of workflow arrows, alter the text in process activity boxes, and change the connections of circuit diagrams.

The Contractor shall provide draft documents for informal review no later than (NLT) two (2) weeks prior to the formal deliverable date to facilitate successful, on-time formal delivery. These draft documents must also be presented in editable, printable formats.

The Contractor shall document all documentation changes and place them under USMC configuration management (CfM).

The Contractor shall divulge all technical details to the Government; the Government retains the rights in technical data produced under this contract as specified in the clauses incorporated herein. The Contractor shall document all designs, configurations, settings, and other data relevant to the technical work performed in the TDPs. The Contractor shall provide additional deliverables in any case where the TDPs and other existing artifacts are not appropriate media for any particular technical details.

All Requests for Change (RFC) must be submitted to the Project Officer before any system changes can be injected into the environment (Training, Zone A, and EITC) and these typically require a two-week lead time to get to the Change Advisory Board (CAB) and receive approval. After CAB approval, the RFC goes to the RDM, which could take an additional two weeks or more. This means that RFCs will have to be drafted and submitted approximately four weeks before a proposed change to the network to meet future Contractor delivery schedules.

1.4.7 **Coordination with Concurrent Efforts**

Conduct of ITSM process training, implementation, installation, configuration, and training of other tools may be accomplished in parallel with other vendors. The Government desires a unified, integrated ITSM solution. The Contractor shall support the Government in achieving this goal by coordinating efforts and schedules with other efforts and vendors through the Government POC. Where conflicts arise, the Contractor shall present them to the Government for adjudication. The Contractor shall support integration by including all design and configuration details in deliverables which become Government property.

When requested by the Government, the Contractor shall allow other Government Contractors to attend all meetings, workshops, conference calls, and training events, and shall review draft documentation related to this task order facilitating an open exchange of information. The Contractor shall support Government-led transition efforts to introduce awardees of other contracted ITSM support tasks into planning and operations.

1.4.8 **Process Adherence**

Although Marine Corps ITSM processes and tools are meant to guide and support the delivery of services by a variety of different programs and organizations, the Marine Corps ITSM team must follow the same guidance in its work on the Marine Corps ITSM system itself. The Contractor shall conform to Marine Corps ITSM processes while carrying out the tasks herein. The Contractor shall work in accordance with the following process restrictions as well as all additional guidance listed in Marine Corps ITSM process documentation:

- Associate IT service-related data with the services in the Marine Corps Service Catalog.
- Document all incidents and incident response activities related to contractor tasks in the USMC Remedy Incident module.
- Make no changes to operational systems, or other systems under ChM control, without a Government-approved RFC which describes that specific change.
- Ensure that the configurations of the processes, tools, and services as related to contractor tasks are documented in the Marine Corps ITSM Configuration Management System (CMS). The CMS includes the USMC Remedy Atrium CMDB, multiple USMC SharePoint sites, and the USMC Definitive Media Library.
- Bundle changes to the ITSM tools suite into thoroughly documented release packages.
- Complete and support all RFC packages for the USMC ITSM tool suite that must go through the Marine Corps ITSM processes.

1.4.9 **SME Skill Set Requirements**

The contractor shall provide Subject Matter Experts SME(s) to support the USMC ITSM Toolset. The

contractor shall identify and provide resumes as part of the initial proposal for SME personnel who have expertise managing, implementing, and operating ITSM support, delivery, and service implementation technologies identified below such as: ITSM Support, Delivery, and Service Implementation.

No single individual is required to be an expert in all areas; however individuals collectively shall be able to provide expertise across all areas.

If, due to an individual's inability to perform the role due to, e.g., illness, death, termination of employment, or for other reasons, the contractor shall substitute the SME with a replacement possessing the requisite experience noted above. The contractor shall provide the Contracting Officer with the substitution notification, including a resume for the proposed individual. Given that this is a Performance Based Requirement, failure of the contractor to provide personnel with the requisite skills necessary to perform the contract may result in breach.

- Incident Management
  - BMC Remedy Incident Management
  - BMC Remedy Service Request Module
- Event Management
  - HP Operations Manager for Windows
  - HP Operations Manager
  - HP Network Node Manager
  - Business Service Manager
- Change Management
  - BMC Remedy Change Management
- Configuration Management
  - HP Tooling (Universal Configuration Management Database/Dependency Mapping Advanced Edition - uCMDB/DDMa)
  - BMC Remedy Atrium CMDB
- Release and Deployment Management
  - HP Tooling (HP Operations Orchestration, HP Server Automation (HPSA), HP Network Automation (HPNA), and uCMDB)
  - BMC Remedy Release Management
  - Microsoft SCCM

- Service Catalog Management
  - BMC Remedy Service Request Module
- Service Request Fulfillment Management
  - BMC Remedy Service Request Module
- Knowledge Management
  - BMC Remedy Knowledge Management
- Problem Management
  - BMC Remedy Problem Management
- Identity and Access Management
  - BMC Remedy Access Management
- Service Level Management
  - BMC Remedy Service Level Management
- Availability Management
  - ITSM HP tools and Service Health Reporter Availability Management
- Capacity Management
  - ITSM HP tools and Service Health Reporter Capacity Management
- Demand Management
  - ITSM HP tools and Service Health Reporter Demand Management
- Non-process specific
  - BMC Remedy SMART Reporting/Analytics
  - BMC Remedy Development
  - BMC Remedy Administration
  - Oracle Database Administrator (DBA)
  - HP Operations Management Tools suite (e.g. BSM) Developers
  - HP BSM Administrator
  - HP SQL Server DBA
  - Microsoft System Center Configuration Manager (SCCM) Administration
  - Training Development Software (e.g. Captivate, Camtasia)

1.4.9.1 SME Personnel

Specific experience with operations and implementation of the following IT disciplines is required:

- Network communication techniques (VPNs, VLANs, MPLs, etc.)

- Network management
- IPv4 and IPv6 configurations, support, and address management
- Cybersecurity
- Network Time Protocol (NTP)
- Domain Name System/Domain Name System Security (DNS, DNSSec)
- Dynamic Host Configuration Protocol (DHCP)
- Simple Network Management Protocol (SNMP)
- Simple Mail Transfer Protocol (SMTP)
- Storage Area Network (SAN)
- Network Attached Storage (NAS)
- Routing protocols (e.g. BGP, IGP, EIGRP, RIP, OSPF, etc.)
- Virtualization
- High Availability (HA)/Disaster Recovery (DR) solutions
- File Services, Storage, Retrieval and Removal
- Directory Services, Management Tools
- Global Address List (GAL) Sharing
- Messaging
- Web/Portal Services
- Print services
- Software distribution/patching
- Business Process Management/Information Technology Services Management (ITSM) Tools
- Information Technology Service Continuity Management/Continuity of Operations Plan (COOP) Tools
- SharePoint Services
- Network Monitoring and Management
- Wide Area Network (WAN)
- Network Communications Infrastructure Hardware, Routers, and Switches
- Asynchronous Transfer Mode (ATM)
- Broad Area Network (BAN)/Local Area Network (LAN)
- Ethernet Standards
- Firewalls
- Access Control Lists (ACLs)
- Demilitarized Zone (DMZ)
- Webmail
- Intrusion Detection Devices (IDS)
- Intrusion Protection Devices (IPS)

- Load Balancing
- Deep Packet Inspection
- Remote Network Monitoring (RMON) and RMON-II
- NetFlow
- Network Access Control & Network Admission Control (NAC)
- Network Address Translation (NAT)/Port Address Translation (PAT)
- Server Management
- Active Directory Domain Controllers
- Information Assurance
- Sustainability

1.4.9.2 SME System Access Requirements

Contractor personnel who will be working on the production systems and supporting live environments shall meet the following criteria:

- Contractor personnel requiring standard system access shall have a fully adjudicated SECRET clearance at the start of their performance.
- Contractor personnel requiring administrative access to systems shall have a fully adjudicated SECRET clearance at the start of their performance.
- Contractor personnel requiring administrative access to systems shall be IAT level II certified at the start of their performance.

1.4.10 **Personnel Access Requirements**

The Contractor shall complete appropriate forms and processes in order to obtain valid access to systems and facilities. The forms and processes include, but are not limited to: System Authorization Access Request (SAAR), access to Operational Directive (OpDir), Marine Corps Certification & Accreditation Support Tool (MCCAST), access badges for MCSC, request for SIPRNet access, Contractor Verification System (CVS), and Joint Personnel Adjudication System (JPAS). The Contractor shall ensure adherence to the requirements listed in DoDI 8500.2 and DOD 8570.01M; specifically, Contractor personnel who will be working on the production systems and supporting live environments are required to have and maintain IAT Level II certification.

They shall conduct initial and annual IA refresher awareness training in accordance with MARADMIN 257/12.

1.4.11 **Code Review**

The vendor will document all code modifications according to a Contractor-supplied standard, approved by the Government.

1.4.12 **Implement, Monitor and Report on Contract Risks**

The Contractor shall implement a risk management process that aligns its assessment methodology with program and contract objectives. Risk reports summarizing the risks and identifying the likeliness and consequences of each risk will be developed and shared with the Government.

2.0 Performance Requirements

2.1 Objectives

The Contractor shall utilize industry best practices for program management of all objectives and associated deliverables. All objectives will need to be considered for both the classified and unclassified network domains.

2.1.1 **Objective 1: Program Management**

The Contractor shall manage delivery of the task order, reporting to the Government ITSM team as stated in the PRS. The Contractor shall provide accurate and timely schedule and performance information throughout the life cycle of the task order.

2.1.1.1 The Contractor shall attend a Government Kick-Off Meeting (or Post Award Conference) within five (5) working days after task order award at or near the greater Quantico, VA area. The purpose of this Kick-Off meeting is to: (1) aid both the Government and Contractor personnel in achieving a clear and mutual understanding of all requirements; and (2) identify and resolve potential problems. It is anticipated that the kick-off meeting will be no more than one work day in duration. It shall include, but not be limited to, an overview of requirements; quality assurance and acceptance procedures; Program Management Plan; personnel and physical security issues; data and deliverable structure or format; and other potential issues or problems. The Contractor shall

provide initial versions of Integrated Master Schedule (IMS), Work Breakdown Structure (WBS), Program Management Plan (PMP), Staffing Plan, and Risk Management Plan (RMP) in accordance with the Deliverables list.

2.1.1.2 NLT 10 working days after the Government Kick-off Meeting, the Contractor shall deliver an updated Integrated Master Schedule (IMS) that encompasses the entire scope of the task order to include Government dependencies. The Contractor shall ensure each non roll-up task shown in the IMS is broken down to not exceed 40 hours in duration. The Contractor shall update the IMS monthly and provide the update as part of each Monthly Status Report (MSR). The Contractor shall make draft updates available to the Government on at least a weekly basis. The Government will ensure integration of organizational efforts from MCNOSC, MARCORSYSCOM, Headquarters Marine Corps Command, Control, Communications, and Computers (HQMC C4), sites, and other stakeholders as required.

2.1.1.3 NLT 20 working days after the Government kick-off meeting, the Contractor shall deliver an updated WBS and Staffing Plan. The Contractor shall ensure each non roll-up task shown in the WBS is broken down to not exceed 40 hours in duration. The Contractor shall update the WBS and Staffing Plan monthly and provide the update as part of each MSR. Include a description of the roles and responsibilities of the Contractor personnel and how they will interface with Marine Corps personnel, as well as a description of the Contractor’s organizational structure and how this structure supports the Marine Corps’ objectives.

2.1.1.4 NLT 30 days after contract award, the Contractor shall provide an updated Risk Management Plan (RMP) and shall establish risk managers that adhere to a sound risk management system and mitigate risk to cost, schedule, and performance through early identification and integration of metrics to monitor task status. The Government will lead the overarching risk management effort. The Contractor shall

participate in the Government risk management system throughout the PoP, to include attendance at Risk Management Board meetings.

2.1.1.5 Throughout the Task Order performance period, the Contractor shall provide management and technical participation in weekly status meetings that provide the Government progress and accomplishments on task, schedule, and any issues. The Contractor shall provide a detailed status report one (1) working day prior to the meeting and detailed minutes to the Government at the conclusion of each meeting.

2.1.1.6 The Contractor shall perform the following tasks in support of meetings necessary to perform and plan the contract tasks:

- Write and submit calendar invitations.
- Record minutes, action items, decisions, and executive summaries.
- Arrange for government bridge phone lines and operate virtual meeting systems such as Defense Collaborative Services (e.g., DCS).
- Prepare, archive and track agendas.

2.1.1.7 The Contractor shall provide MSRs, which shall include management, technical, and Task Order execution profiles. The Contractor shall provide an updated Contractor’s Progress and Status Report, and action items with each MSR.

2.1.1.8 The Contractor shall ensure that work under this task order is managed efficiently. The Contractor’s Program Manager shall be the single point-of-contact to ensure effective program management, direction, administration, quality assurance, and control of the task order.

2.1.1.9 Engineering Design/Documentation

The Contractor is responsible for solution designs and supporting USMC enterprise engineering efforts including supporting system enhancement, updating, and validation of design documentation, instructions and procedures, and supporting documentation for enterprise solutions. All documentation must be

managed under strict configuration controls. Documentation shall be technically and procedurally sufficient to allow a third party to validate and/or install and configure the specified systems within the MCEN. Systems Administration and Operational guides shall be in accordance with Industry Best Practices.

Deliverables from each of the engineering efforts include professional level technical documentation including decision and point papers and complete and accurate diagrams. The Contractor shall support the creation and enhancement of the following required documentation.

Design documentation for enterprise solutions and systems should be based on and must follow the existing Marine Corps Documentation as stated in section 1.4.6. Any additional template that may be necessary for additional documentation must be approved by the Government prior to creation or enhancement.

For each engineering change to the ITSM tool suite, the Contractor shall consult the EEVE Engineering Peer Review (EPR) regarding the engineering documentation required to appropriately document the change.

The Contractor shall provide draft and final engineering documentation in IS&I engineering document format to the EPR, through the EP&I Engineering Technical Lead, for approval during system enhancement design and prior to implementation.

The EP&I Engineering Technical Lead (Government Technical Lead) shall submit the EPR approved documents to the Enterprise Solutions Board (ESB) to gain approval for enterprise solution acceptance. The Contractor shall coordinate with EP&I Engineering Technical Lead (ETL) for posting to the DML.

The contractor shall support successful completion of SETR events within the established timeframe.

The contractor shall submit documents for USMC review IAW Technical Review Action Plan (TRAP).

The scope of IS&I engineering documentation includes:

- DEV400 Solution Architecture and Concept of Operations
- DEV401 Detailed Technical Design
- DEV403 Detailed Configuration
- DEV405 Solution Components
- DEV406 Engineering and Operating Guidelines
- DEV408 Requirements Document
- DEV409 Functional Test Plan
- DEV410 Implementation Guide
- DEV411 Data Architecture
- Requirements Traceability Matrix
- Test Plans (including supporting test cases, test scripts and use cases)
- Diagrams and technical drawings (including logical, physical, wiring, data flow, and topological)
- Concept of Operations (CONOPS)
- DoD Risk Management Framework (RMF) documentation including:
  - Continuous Monitoring Strategy Document
  - Security Assessment Plan (SAP)
    - Hardware & Software lists
    - Ports, Protocols, and Services Document
    - Interfaces & Interconnections Document
    - ATO Boundary Document
    - Data Flow Diagram
    - Security Controls
    - Test Plan
    - Continuity Plan
  - Security Assessment Report (SAR)
    - Finalized Continuous Monitoring Plan
    - Finalized Security Controls
    - Source Code Review
    - Risk Assessment Report (RAR)

2.1.1.10 Quality Control

The Contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's quality control program is the means by which the Contractor assures

work complies with the requirements of the contract. The Contractor shall implement a quality assurance process that will improve all products (software, CDRLs, etc.) delivered to the Government. The Contractor's Quality Control effort shall be described in accordance with the QAPP and the CDRL and shall address the areas identified in the Performance Requirements Summary.

2.1.1.11 Quality Assurance

The Government shall evaluate the Contractor's performance under this contract in accordance with the Performance Requirements Summary and Quality Assurance Surveillance Plan (QASP). The QASP focuses on what the Government must do to ensure that the Contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

The Contractor's systems engineering, quality assurance, and quality control efforts shall comply with Government policy and instructions and be reflected in the Contractor's ITSM O&S efforts to ensure existing and new/enhanced capabilities meet the Government's objectives for zero defects.

The Contractor's quality assurance program shall provide a total quality management system approach to the Marine Corps ITSM effort and shall include program and technical management, quality assurance, quality control, and performance management to achieve the control of product and service quality throughout the task performance.

The Contractor's quality control procedures shall address the areas identified in the Performance Requirements Summary. The Contractor shall develop a Quality Assurance Program Plan (QAPP) in accordance with the CDRL.

2.1.1.12 Government Surveillance

The Contracting Officer Representative (COR) will function as the Technical Representative for this task. Technical Representative Authority will be limited to administering specific technical aspects of the contract. The Technical Representative will not provide direction that is outside the scope of

responsibilities delineated under this task order. The designated individual will:

- Maintain a detailed knowledge of the technical requirements of the contract.
- Document Contractor performance in accordance with the PRS
- Identify and immediately forward notifications of deficient or non-compliant performance to the KO.
- Approve priorities of support, resources, and associated schedules.

2.1.2 **Objective 2: ITSM Tool Suite Operations and Maintenance**

The Marine Corps seeks technical support to operate and maintain the current ITSM tool suite that enables the Marine Corps to deliver IT service management functions to its user base. This objective describes the sustainment activities required for the daily operations and maintenance of the ITSM tool suite.

The ITSM tools and related infrastructure include virtual machines, physical servers, database servers, application instances, and supporting software such as plug-ins and middleware on both unclassified and classified networks. The MCNOSC has daily operational responsibilities for the ITSM toolset which is hosted from the EITC located in Kansas City, MO but maintained remotely from Quantico, VA.

The Contractor is not responsible for the maintenance of the MCEITS hosting infrastructure on which many of the ITSM tool components depend. However, the Contractor shall conduct operations and sustainment activities related to the hosted ITSM applications including databases, operating systems, and application level patching. Upon identifying a need for ITSM tool suite maintenance, the identifying party (Government or Contractor) will be responsible for documenting the need for issue prevention, issue resolution, or toolset modification via the USMC BMC Remedy ticketing system.

The Marine Corps requires that release packages for the ITSM toolset be certified and accredited per security related guidelines provided in section 6.2 of this document. The Contractor shall also perform the subtasks identified below:

2.1.2.1 Information Security

- Provide security requirements identification, analysis, allocation, and tracking support utilizing DoD Risk Management Framework (RMF) documentation as required. Mitigate any security related issues or incidents that may introduce security risks or that do not comply with existing security related policies, regulations, or standards in order to maintain an ATO for all components of the Marine Corps ITSM system.
- The Contractor shall ensure that the ATO is retained through maintenance and operation activities and USMC IA policy changes.
- Develop and update all engineering documentation and artifacts for accreditation packages, scanning, and remediation of findings.
- Provide required security SCAN reports and POA&Ms within establish timeframes.
- Submit updates to existing accreditation packages to accompany all changes to components within the ZONE A and EITC enclaves.
- Create new accreditation packages for all components outside the ZONE A and EITC enclaves, supported by the Government IA staff where Government approvals and inputs are required by policy as needed.

2.1.2.2 General System Requirements. The Contractor shall:

- Document all changes under the scope of this task and place them under USMC configuration management (CfM). The Contractor shall use strict CfM for all hardware, software, documentation, and deliverables.
- Acknowledge Advanced Technical Problems/Issues and respond to the related tickets within two (2) hours of verbal notification and/or ticket creation by MCNOSC. A 2-hour response time is expected during the regular Government business hours. However during major incidents, live operational support may include outside business hours to support urgent break fixes. The response should come from a Contractor employee. The Contractor's relevant technical SME that has acknowledged the related incident/problem ticket must provide verbal or written

notification to the Government operational POC. The contractor shall provide written updates (including summary of problem/issue or requirement, actions taken in the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion) to the Government operational POC until the problem/issue is resolved. These written updates shall be provided, at a minimum, for 95% of all such occurrences. The contractor shall maintain the ITSM toolset availability at 98% (based on unplanned downtime). Availability issues caused by USMC actions are not in the scope of this objective. Advanced Technical Problems/Issues data shall be compiled in the weekly and monthly status reports.

- Under the federal information security Risk Management Framework, the ITSM tools are classified for Confidentiality, Integrity, and Availability as Medium-Medium-Low. The Contractor shall perform restoration services, within established timeframes 98% of the time each month, on these tools once notified through verbal notification or ticket creation by MCNOSC. The Recovery Time Objective (RTO) Threshold is eight (8) hours (Monday through Sunday; Government Holidays included)/ Objective two (2) hours.
- Provide ad-hoc reports within five (5) working days of the request.
- **Perform maintenance and sustainment activities as required to ensure the following:**

o The ITSM tool suite continues to enable the authorized user to create, read, update, and delete action workflows including at a minimum sending email notifications upon Service Level Agreement/Operating Level Agreement (SLA/OLA) monitoring targets for system and subsystem entries.

o The ITSM tool suite continues to enable the authorized user to reflect system and subsystem entry point of contact (POC) details within the associated subsystem entry including at a minimum

first name, last name, middle name or initial, and rank/title data elements.

- The ITSM tool suite continues to enable the authorized user to reflect the information (email address, location, and phone number) necessary to contact the originator, submitter, owner and other POCs for a given system and subsystem entry.
- The ITSM tool suite continues to enable the authorized user to perform search-based population of system POC attribute fields within system entries.
- The ITSM tool suite continues to enable the authorized user to identify a specific individual as a Very Important Person (VIP).
- The ITSM tool suite continues to incorporate design features as necessary to enable the tracking and prioritizing entries which are created by or on the behalf of a VIP.
- The ITSM tool suite continues to incorporate design features as necessary to allocate a unique identifier to each system and subsystem entry at the time of entry creation.
- The ITSM tool suite continues to enable the authorized user populate foundation information into Foundation Data attribute fields within each system and subsystem entry.
- The ITSM tool suite continues to enable the authorized user to reflect types and categories for a given system or subsystem component as part of the associated system or subsystem entry.
- The ITSM tool suite continues to enable the authorized user to view system or subsystem entries including at a minimum attribute field content and associated subsystem entry relationships.
- The ITSM tool suite continues to incorporate design features as necessary to enable the import of data utilizing common formats, including at a minimum .csv and .xlsx.
- The ITSM tool suite continues to incorporate design features as necessary to enable the export

of data utilizing common formats, including at a minimum .csv and .xlsx.

- The ITSM tool suite continues to enable the authorized user to create subject/overview and summary information for a given system or subsystem entry as part of the associated system or subsystem entry.
- The ITSM tool suite continues to enable the authorized user to create comments, work activities, updates, assignments, and escalations for a given system or subsystem entry as part of the associated system or subsystem entry.
- The ITSM tool suite continues to enable the authorized user to create comments which may only be edited by role based authorization.
- The ITSM tool suite continues to maintain a history of logged comments within each system or subsystem entry.
- The ITSM tool suite continues to enable the attachment of documentation for system and subsystem entries.
- The ITSM tool suite continues to enable the authorized user to create and publish scheduled and ad hoc real-time and historical graphical reports by querying system-wide and discreet subsystem attribute content, including at a minimum entries, entry attributes, system logs, and entry associations.
- The ITSM tool suite continues to enable the authorized user to create and publish scheduled reports in a consolidated, real-time graphical presentation of targeted periods and historical trends by querying system-wide and discreet subsystem attribute content, including at a minimum entries, entry attributes, system logs, and entry associations.
- The ITSM tool suite continues to enable the authorized user to distribute system and subsystem based customer satisfaction surveys.
- The ITSM tool suite continues to enable role and/or attribute-based access to system and subsystem entries and subsystem entry content

through defined, hierarchical location and personnel management groupings.

- The ITSM tool suite continues to enable system and subsystem access control audits, reporting, and remediation of deviations.
- The ITSM tool suite continues to enable the authorized user to create, read, update, and delete system and subsystem workflows for the handling of system and subsystem entries in support of system and subsystem activities.
- The ITSM tool suite continues to enable the sequential logging of system and subsystem entry creations, deletions, and modifications by storing modification details including at a minimum action summary, acting user, date, and time of the modification.
- The ITSM tool suite continues to enable the authorized user to populate lifecycle attribute fields within a given system or subsystem entry with lifecycle statuses specific to that type of system or subsystem entry.
- The ITSM tool suite continues to enable the authorized user to modify system and subsystem attributes including at a minimum entry and entry attribute field identifiers, labels and content to align with system, subsystem, and organizational naming conventions and terminology.
- The ITSM tool suite continues to enable the authorized user to create system or subsystem templates to auto-populate system or subsystem entries based on commonly used subsystem models.
- The ITSM tool suite continues to enable the authorized user to relate system or subsystem entries to multiple other system or subsystem entry, including at a minimum one-to-one, one-to-many, and many-to-one entry relationships.
- The ITSM tool suite continues to enable the authorized user to access self-help capabilities to create a given set of system or subsystem entries.

- The ITSM tool suite continues to enable the authorized user to access a given set of self-help knowledge information.
- The ITSM tool suite continues to enable the authorized user to perform full-text and attribute based searches for system and subsystem entries by through a combination of system or subsystem entry attributes.
- The ITSM tool suite continues to enable the authorized user to create and deliver system notifications to inform users regarding outages, degradations, and announcements.
- The ITSM tool suite continues to enable the retention of historical notifications for reporting and printing.
- The ITSM tool suite continues to enable alerts (including at a minimum integration with e-mail) based on entry assignment, status, modification, impact, priority, visibility, outcome, or need for action.
- The ITSM tool suite continues to enable assignment of system and subsystem entries to authorized user defined groups or individuals.
- The ITSM tool suite continues to enable workflow for the escalation of system and subsystem entry assignments.
- The ITSM tool suite continues to implement field-based data validation upon data creation/modification within a system entry.
- The ITSM tool suite continues to enable receipt of replies to email notifications and to log those replies within entry comment logs.
- The ITSM tool suite continues to enable the recording of Uniform Resource Locator (URL) hyperlinks.
- The ITSM tool suite continues to maintain and report authorized user defined grouping of system and subsystem entries by entry lifecycle stage(s).
- The ITSM tool suite continues to enable the storage and display of individual and

consolidated customer satisfaction survey results.

- The ITSM tool suite continues to enable the authorized user to implement custom entries in support of system and subsystem workflow.
- The ITSM tool suite continues to enable the authorized user to create, read, update, and delete custom metadata as data attributes for ITSM system or subsystem entries.
- The ITSM tool suite versioning remains up to date in relation to IA regulations and vendor support.

2.1.2.3 Remedy Upgrade

- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite remains updated with current software versioning. The Contractor shall upgrade the existing Remedy 8.x solution to version 9.1.0.2 (or later) to include BMC Smart IT functionality. The Contractor shall perform the update in all USMC ITSM toolset environments.
- The Contractor shall ensure that the ATO is renewed/retained for new system versions and all effected environments.
- The Contractor shall document the system upgrade as an engineering change utilizing the documentation and review requirements listed in Section 2.1.1.9. As part of required engineering documents, the Contractor shall develop a test plan (including supporting test cases, test scripts and use cases) to verify functionality of upgraded features and ensure that previous out-of-the-box and custom functionality is retained.
- The Contractor shall design, develop and maintain a new equipment training (NET) package. All training materials shall meet the training materials requirements listed in Section 2.1.3.
- The Contractor shall conduct NET prior to solution deployment.

2.1.2.4 Incident Management (IM)

- The Contractor shall monitor the ITSM toolset queue and respond to requests in the USMC BMC

Remedy ticketing system. Document all tickets, with detailed resolution steps, for every ticket that is escalated.

- The Contractor shall work as part of the Incident Resolution team (identified by the Watch Officer in accordance with documented processes and procedures) to ensure restoration of services as quickly as possible for all major incidents associated with the ITSM toolset.
- The Contractor shall keep the MCNOSC S-3/ Network Common Operational Picture (NetCOP) section informed of status on all tickets through proper ticket documentation, daily status reports, email, and direct communications.
- **The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to do the following:**

o To enable the authorized user to create, read, update, and delete incident entries (as defined in this specification).

o To ensure the ITSM tool suite continues to enable the authorized user to create an incident entry on behalf of another user. The Contractor shall enable the authorized user to log user information for both the user creating the entry and the user on the behalf of whom the entry was created.

o To ensure the ITSM tool suite continues to enable the authorized user to record the method that should be used to contact the customer reporting a given incident as part of the associated incident entry.

o To ensure the ITSM tool suite continues to enable the authorized user to record incident resolution data for a given incident as part of the associated incident entry, including at a minimum resolution action, date and time.

o To ensure the ITSM tool suite continues to enable the authorized user to record the source of a given incident (event trigger, person, group), including at a minimum how the incident was reported as part of the associated incident entry.

- To ensure the ITSM tool suite continues to enable the authorized user to reflect the impact and urgency of a given incident as part of the associated incident entry.
- To ensure the ITSM tool suite continues to enable the calculation of incident priority based on the impact and urgency assigned to a given incident as part of the associated incident entry.
- To ensure the ITSM tool suite continues to enable the authorized user to manually override the assigned priority for a given incident as part of the associated incident entry.
- To ensure the ITSM tool suite continues to enable the authorized user to reflect a given incident as a Major incident, Commander's Critical Information Requirement (CCIR), and Friendly Force Information Requirements (FFIR) as part of the associated incident entry.
- To ensure the ITSM tool suite continues to enable the authorized user to produce reports in support of identifying and analyzing incident trends.
- To ensure the ITSM tool suite continues to enable monitoring of incident entries in support of SLA and OLA targeting. The Contractor shall incorporate design features as necessary to enable responses to SLA/OLA breaches.

2.1.2.5 Request Fulfillment (RqF)

- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to maintain the BMC Remedy SRM Module to support templated IT requests as required by the RqF process based on the existing Marine Corps process guide and FDD for RqF.
- The Contractor shall work with the SCM team to define criteria around RqF for each service and determine how the requested service will be fulfilled through the BMC Remedy SRM Module.
- The Contractor shall enhance and expand existing service request workflows in support of additional service catalog offerings.

- The Contractor shall incorporate USMC regional request fulfillment workflows needed to support enterprise services at the regions within the enterprise ITSM toolset.

- **The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to :**

  - Enable the authorized user to visualize the set of service requests and their associated service catalog entries.
  - Enable the authorized user to associate a given service request to one or more service catalog entries as part of the associated service catalog entry.
  - Enable the authorized user to record approvals and rejections of a given request as part of the associated request entry.
  - Enable the authorized user to produce reports in support of identifying and analyzing request trends.

2.1.2.6 Service Catalog Management (SCM)

- The Contractor provide the identification and integration of existing services which could be offered within the USMC On-Line Enterprise IT Service Catalog.

- **The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to :**

  - Enable modification and expansion of the content of the existing Marine Corps Service Catalog contained in the BMC Remedy SRM module (unclassified and classified network domain components) such that it contains all end-user facing services corresponding to services from MCIENT core component capabilities.
  - Enable continued alignment of the service mappings of CIs to respective Business and Technical services using the BMC Remedy SRM and CMDB tools.
  - Enable creation of the service mappings following a relational, object-oriented configuration data

model contained in the Marine Corps ITSM toolset and referenced in the MCIENT CMP. The CMP and configuration data model will be provided as part of the GFI.

- Enable the authorized user to create, read, update, and delete service linkage information among interrelated services as part of the associated service catalog entries.
- Enable the authorized user to create, read, update, and delete linkage information between a given service catalog entry and associated service request entries.
- Enable the authorized user to identify SLAs associated with IT services defined in the service catalog to include identifying the condition that no service level agreement is associated with a given IT service.
- Enable the authorized user to record the performance results of a given IT service against its associated service level agreements as part of the associated service catalog entry.
- Enable the authorized user to record the business case of a given IT service as part of the associated service catalog entry.
- Enable the authorized user to create and limit user access to view and modify specific services or groups of services and the associated service catalog entry attributes.
- Enable the authorized user to visualize the set of service catalog entries and their associated service requests.
- Enable the authorized user to reflect that a given service is provided by a third party as part of the associated service catalog entry.
- Enable the authorized user to record the service provider information including at a minimum name and service ordering contact information as part of the associated service catalog entry.
- Enable the authorized user to record the service warranty information for a given service as part of the associated service catalog entry.

- Enable the authorized user to create the service utility information for a given service as part of the associated service catalog entry.
- Ensure the authorized user is able to record agreed service hours as part of the associated service catalog entry.
- Ensure the authorized user is able to create relationships among user facing services, organizational services, technical services and capabilities as part of the associated service catalog entry.
- Ensure the authorized user is able to display graphical relationships among user facing services, organizational services, technical services and capabilities.

2.1.2.7 Change Management (ChM)

- **The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to :**

- Enable the authorized user to create, read, update, and delete changes entries (as defined in the specification).
- Enable the authorized user to record approvals and rejections of a given change request as part of the associated change entry.
- Enable the authorized user to record business impact and urgency indicators for a given change request as part of the associated change entry.
- Enable the authorized user to identify the business and technical requirements associated with a given change as part of the associated change entry.
- Enable the authorized user to create, read, update, and delete SLA and OLA monitoring targets in regard to change entries.
- Enable the authorized user to manage and maintain a schedule of changes through the association of change entries that have been approved for implementation.

2.1.2.8 Service Asset and Configuration Management (SACM)

- The Contractor shall provide Asset Administration Support for individual and mass CI generation and population, CI auditing and reporting activities as requested by asset management teams, and establishment and changes to BMC Remedy foundation data in support of asset administration.

- **The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to :**

  - Support discovery of CIs and map their relationships in BMC Remedy that underpin services operating in the Marine Corps unclassified and classified network domains.
  - Maintain CI data in HP uCMDB and BMC Atrium CMDB following applicable ITSM processes, the MCIENT CMP, and the configuration data model.
  - Include warranty and license information for all CIs as well as relationships of dependent and associated CIs.

- **The Contractor shall perform maintenance and sustainment activities as required to:**

  - Create software license certificates and relate those certificates to software contract CIs and asset discovery data.
  - Ensure the ITSM tool suite continues to ensure that CMDBs support change impact assessments, incident resolution, and change control.

- **The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to:**

  - Ensure that the BMC Remedy Atrium CMDB is integrated with the CI data discovered by the various CI discovery tools (SCCM, HP UD, NNMi, HP uCMDB) for automated data population based on attribute discovery.
  - Enable the authorized user to create, read, update, and delete configuration item (CI) entries.

- Enable the authorized user to reflect CI classification categories for a given CI as part of the associated CI entry.
- Enable the authorized user to reflect CI attributes for a given CI as part of the associated CI entry. The attributes shall include: Identifier, CI Owner details, People/Support Groups, Contracts, Asset Specifications, Operational Categories, Product Categories, Relationships, Location, Lifecycle Data, In-service Dates, Financing Source Identifier, Physical/Virtual status.
- Enable the authorized user to create, read, update, and delete static Foundation Data including at a minimum baselined hardware and software vendor and model specifications, hierarchical location and personnel management groupings, entry lifecycle statuses, operational and product based categorizations, and personnel records.
- Enable the authorized user to reflect the static Foundation Data elements for a given subsystem component as part of the associated system or subsystem entry.
- Enable the authorized user to reflect change requests associated to a given CI through integration of associated change entries and CI attributes as part of the associated CI entry.
- Enable the authorized user to perform modifications to multiple CI entries simultaneously through a single graphical interface.
- Enable the authorized user to perform the mass validation, normalization, and import of service asset data into new CI entries using standardized template uploads.
- Enable the integration of external discovery tools to perform CI entry creation and update via data retrieval or receipt, validation, normalization, and attribute mapping and assignments.
- Enable the authorized user to display simplified (single) and complex (multiple) graphical

representations of a given CI and the associated CI attributes and relationships.

- Enable the identification of definitive CI data sources and the update of CI entries with CI data elements captured by USMC discovery tools.
- Enable integration with existing USMC asset and configuration management systems to provide the authorized user access to external configuration data.
- Enable the authorized user to configure subsystem workflow as necessary to enable CI entry integration with the USMC business processes for service asset procurement, replacement, and archival including at a minimum contract CI management, CI mass imports, service asset and contract CI relationship mapping, non-discoverable CI attribute population, and the transfer of CI attribute mapping upon asset technical refresh.

- The Contractor shall enable the authorized user to create, read, update, and delete data correlations which enable the alignment of a given discovery tool data element to a corresponding CI entry data element.
- The Contractor shall enable the authorized user to create, read, update, and delete programmable logic to determine if conflicting data elements should be updated or ignored during receipt of data elements from external discovery tools.
- The Contractor shall enable the authorized user to create, read, update, and delete scheduled and ad hoc data integration activities to control the delivery and receipt of data elements from external discovery tools.
- The Contractor shall support the execution of and ensure the ITSM toolset continues to accept imports of CI data reported at the enterprise Staging and Warehousing facility and is imported into the Atrium CMDB through automation.

2.1.2.9 Release and Deployment Management (RDM)

- **The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to:**
  - Enable the authorized user to validate the success of a given release deployment as part of the associated release entry.
  - Enable the authorized user to manage and maintain a schedule of releases that have been scheduled for deployment.
  - Enable the authorized user to record approvals and rejections of a given deployment as part of the associated release entry.
  - Enable the authorized user to specify workflow for tracking Technical Delivery Lifecycle (TDLC) initiatives through the TDLC lifecycle.
  - Enable the authorized user to record the TDLC initiative attributes including at a minimum technical review outcomes, related system and subsystem entries, TDLC documentation, and initiative points of contact.
  - Enable the authorized user to create, read, update, and delete TDLC entries.
  - Enable the authorized user to record approvals and rejections of a given deployment as part of the associated TDLC entry.
  - Enable the authorized user to create, read, update, and delete SLA and OLA monitoring targets in regard to TDLC entries.
  - Enable the authorized user to create, read, update, and delete SLA and OLA monitoring targets in regard to release entries.

2.1.2.10 Knowledge Management (KM)

- The Contractor shall enable the authorized user to analyze raw knowledge assets, consequential information and data for accuracy and usefulness.
- The Contractor shall enable the authorized user to identify and reflect the expected user community for a given knowledge entry as part of the associated knowledge entry within BMC Remedy.

- The Contractor shall enable the authorized user to search and retrieve knowledge articles by keywords, subject, owner, and date within BMC Remedy.
- The Contractor shall enable the authorized user to record the reason for a given knowledge entry to exist as part of the associated knowledge entry within BMC Remedy.
- The Contractor shall enable the authorized user to create, delete or archive knowledge information as knowledge entries within BMC Remedy.
- The Contractor shall enable the authorized user to record data and information from external suppliers as part of the associated knowledge entry within BMC Remedy.
- The Contractor shall enable the authorized user to record relevant regulatory/statutory information as part of the associated knowledge entry within BMC Remedy.

2.1.2.11 Problem Management (PbM)

- **The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to:**
  - Enable the authorized user to create, read, update, and delete incident entries (as defined in this specification).
  - Enable the authorized user to record the source of a given problem (event trigger, person, and/or group) as part of the associated problem entry.
  - Enable the authorized user to record the symptoms of a reported fault as part of the associated problem entry.
  - Enable the authorized user to reflect the impact and urgency of a given problem as part of the associated problem entry.
  - Enable the calculation of problem priority based on the impact and urgency assigned to a given problem as part of the associated problem entry.

- Enable the authorized user to manually override the assigned priority for a given problem as part of the associated problem entry.
- Enable the authorized user to identify and record known errors (problems with an identified root cause).
- Enable the authorized user to record problem resolution data for a given known error as part of the associated problem entry, including at a minimum sequential diagnostic activities.
- Enable the authorized user to identify and record work-arounds to problems and known errors as part of the associated problem entry.
- Enable the authorized user to produce reports in support of identifying and analyzing problem trends.
- Incorporate design features as necessary to enable monitoring of problem entries in support of SLA and OLA targeting.
- Incorporate design features as necessary to enable responses to SLA/OLA breaches.

2.1.2.12 Identity and Access Management (IdAM)

- The Contractor shall enable the authorized user to store documentation supporting user and system access, including at a minimum System Account Access Requests (SAAR), Tool Access Requests (TAR), System Request entries, Access Control Lists (ACL), Rights Registries, and access approvals/denials.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to manage the receipt off access related requests from Request Fulfillment and Change Requests.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to create, read, update, and delete access entries.

- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to access identity data in support of access control decisions.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to create, read, update, and delete SLA and OLA monitoring targets in regard to access entries.
- The Contractor shall enable the authorized user to identify role-based access conflicts across USMC IT systems.
- The Contractor shall incorporate design features as necessary to enable the integration of user-specific identifier technology to verify user identity for USMC IT system and service access, forensics, auditing and reporting.

2.1.2.13 Service Level Management (SLM)

- The Contractor shall incorporate design features as necessary to enable the authorized user to create, read, update, and delete SLAs, OLAs, and underpinning contracts (UC) as service level entries.
- The Contractor shall incorporate design features as necessary to enable the authorized user to relate one or more service level entries to a given service catalog entry as part of the associated service catalog entry.
- The Contractor shall incorporate design features as necessary to enable the authorized user to record service provider details as part of the associated service level entry.
- The Contractor shall incorporate design features as necessary to enable the authorized user to record customer details including, at a minimum, contacts and location details as part of the associated service level entry.
- The Contractor shall incorporate design features as necessary to enable the authorized user to

record agreed service hours as part of the associated service level entry.

- The Contractor shall incorporate design features as necessary to enable the authorized user to record common SLA data, including at a minimum, agreement date, scope, and contacts as part of the associated service level entry.
- The Contractor shall incorporate design features as necessary to enable the authorized user to record service level requirement (SLR) details as part of the associated service level entry.
- The Contractor shall incorporate design features as necessary to enable the authorized user to record each service level target (SLT) details as part of the associated service level entry.
- The Contractor shall incorporate design features as necessary to enable the authorized user to create, read, update, and delete SLA and OLA monitoring targets in regard to system entries.
- The Contractor shall incorporate design features as necessary to enable the authorized user to escalate subsystem entries associated with a given service level entry based on associated SLTs.
- The Contractor shall incorporate design features as necessary to enable the authorized user to reveal and assess potential and existing gaps between target and actual service delivery or service level performance.
- The Contractor shall incorporate design features as necessary to enable the authorized user to produce Service Level Achievement Monitoring (SLAM) charts to monitor service achievements against SLAs.

2.1.2.14 Event Management (EM)

- The Contractor shall monitor Enterprise Monitoring Tier II Remedy queue and resolve event-related incidents as able. Monitor and maintain awareness of regional tickets and items of concern.
- The Contractor shall develop, maintain and evaluate reports of the MEMS network event management solutions and services.
- **The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to:**
  - Enable the authorized user to record and retain historical event data as event entries.
  - Enable the authorized user to record details for a given event including at a minimum device identity, component concerned, type of event state, date and time as part of the associated event entry.
  - Enable the notification and escalation/de-escalation of event alerts based on authorized user definable conditions.
  - Enable filtering of events by authorized user definable informational, warning, and exception event conditions.
  - Enable the correlation of events through the assessment of authorized user definable event criteria and rules.
- The Contractor shall assist the government Event Management team in defining views of events related to the HP Operations Management tool suite and the BMC Remedy suite to be monitored. The Contractor shall implement defined event views.
- The Contractor shall assist the government Event Management team in defining thresholds for monitoring ITSM tools to ensure compliance with availability goals. The Contractor shall implement defined thresholds for monitoring.

- The Contractor shall evaluate and make recommendations for design implementation and integration steps and processes for management and monitoring tools.
- The Contractor shall conduct planning and implementation of event monitoring and management for new or updated IT services using existing ITSM tools. The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to produce reports in support of identifying and analyzing event trends.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to incorporate design features as necessary to execute responses to triggers and/or events based on authorized user definable conditions.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to perform both host-based and remote discovery, monitoring, data collection, and management capabilities in support of event management operations across the Open Systems Interconnection (OSI) model.

2.1.2.15 Continual Service Improvement (CSI)

- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to create, read, update, and delete system, subsystem and service metrics as continual service improvement (CSI) reports pertaining to ITSM system and subsystem entries, including at a minimum entry attributes, entry change history, and entry associations in order to facilitate the measurement of technology components, processes and services.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to access a base-line set of out of the box canned and ad hoc reporting

capabilities that do not rely on a third party report generator, including at a minimum the ability to export reports into .csv, .txt, .xls, .htm formats, and to hyperlink report content for direct access to system and subsystem entries.

- The Contractor shall provide support to generate reports from uCMDB.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to schedule reports at configurable intervals.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to specify data requirements and integrate analytical logic into CSI reports.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to specify the presentation of CSI report information.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to enable the authorized user to request, collect, and analyze customer satisfaction input for each subsystem and service area.
- The Contractor shall perform maintenance and sustainment activities as required to ensure the ITSM tool suite continues to define, develop, document and implement metrics and tools to capture metrics, as directed, for all E-ITSM process areas.
- The Contractor shall perform activities as required to provide and execute a strategy for responding to reporting requests within the E-ITSM tool suite based on new reporting requirements and existing legacy reports.

2.1.3 **Objective 3: Enhancement of ITSM Training Materials**

As operations and maintenance activities occur which alter the interfaces and/or workflows of the ITSM Tools Suite, support is required to update and mature existing ITSM Process New Equipment Training (NET) packages and individual training materials. Materials requiring updates include computer based training (CBT), Procedures/Work Instructions (PWI), Just-In-Time videos (JIT), Job Aids, and Knowledge Articles for the Marine Corps ITSM processes, workflows, and ITSM tool suite. Existing training materials will be provided as GFI. Updates to training materials shall follow the Marine Corps Systems Approach to Training (SAT) Users Guide for classroom and self-paced instruction and MarineNet Courseware configuration and enhancement Technical Requirements for CBTs. Each shall be Shareable Content Object Reference Model (SCORM) Compliant and also have the ability to be hosted in a Learning Management System (LMS). The Contractor shall provide the code/editable version of each NET package and training component. The Contractor shall assist the government in configuration and enhancement of MarineNet hosting submission documentation and process.

2.1.3.1 The Contractor shall mature and update the training documentation to coincide with major changes to ITSM tools suite and processes such as tools upgrade, major ITSM process improvements, and tool enhancements.

2.1.3.2 The Contractor shall develop new training documentation such as CBTs, Just in Time Videos, and Job Aids as necessary to coincide with major changes to ITSM tools suite and processes such as tools upgrade, major ITSM process improvements, and tool enhancements.

2.1.3.3 The Contractor shall conduct training as described below in section 2.1.3.4 for changes to ITSM tools suite and processes such as tools upgrade, major ITSM process improvements, and tool enhancements.

2.1.3.4 The Contractor shall provide virtual training to USMC operators, maintainers, and stakeholders. The Contractor shall plan (in conjunction with the COR), host, and conduct virtual training sessions for the ITSM tools suite modules, custom applications, and ITSM processes

not to exceed seven (7) individual two (2) hour sessions per quarter.

2.1.4 **Objective 4: ITSM Toolset Training Environment**

The Marine Corps seeks an advanced ITSM toolset technical problem prevention and problem resolution capability for the ITSM training environment. The Marine Corps also seeks an advanced ITSM toolset modification capability for the ITSM training environment.

MCNIS has daily operational responsibilities for the training stack ITSM toolset currently located in NGEN West at MCTSSA, Camp Pendleton, CA. The tools and related infrastructure include virtual machines, physical servers, database servers, application instances, and supporting software such as plug-ins and middleware. Expertise in BMC toolsets and familiarity with HP tools is required.

2.1.4.1 The Contractor shall provide ITSM tools technical support to the MCTSSA Government lab manager in maintaining the ITSM training stack so it is up and available to conduct ITSM training and User Acceptance Testing.

2.1.4.2 The Contractor shall ensure the training environment mirrors the production environment in terms of application configuration. The Contractor shall work with SACM and CMDB teams to ensure that the training environment is populated and kept up to date with configuration data from the production environment.

2.1.4.3 The Contractor shall maintain CfM including hardware, software, networking, and operational procedures for the training environment.

2.1.4.4 The contractor shall acknowledge Advanced Technical Problems/Issues and respond to the related tickets within two (2) hours of verbal notification and/or ticket creation by MCNOSC. The response should come from a Contractor employee. The Contractor's relevant technical SME that has acknowledged the related incident/problem ticket must provide verbal or written notification to the Government operational POC. The contractor shall provide written updates (including summary of problem/issue or requirement, actions taken in the last 24 hours, actions planned for the next 24

hours, and estimated date/time of completion) to the Government operational POC until the problem/issue is resolved. These written updates shall be provided, at a minimum, for 95% of all such occurrences. Advanced Technical Problems/Issues data shall be compiled in the weekly and monthly status reports.

2.1.5 **Objective 5: ITSM Toolset Configuration and Enhancement Environment**

The Marine Corps seeks the establishment of an advanced ITSM toolset enhancement capability implemented as an ITSM tools configuration and enhancement Environment. The Marine Corps also seeks an ITSM tools configuration and enhancement Environment sustainment capability for the ITSM tools configuration and enhancement Environment upon establishment.

2.1.5.1 The Contractor shall establish the ITSM tools configuration and enhancement Environment within the MCSC Enterprise Engineering and Verification Environment (EEVE) at MCSC, Quantico, VA utilizing EEVE hardware, software, and infrastructure. The ITSM tools configuration and enhancement Environment will include virtual machines, physical servers, database servers, application instances, and supporting software such as plug-ins and middleware.

2.1.5.2 The Contractor shall perform all ITSM tools configuration and enhancement Environment Work implementation and changes utilizing the existing EEVE Change Management process. The Contractor shall describe the modifications or enhancements, if any, of the tools configuration and enhancement environment required allowing it to fulfill its mission of providing an effective tools configuration and enhancement environment for the EITC production environment.

2.1.5.3 The Contractor shall perform operational and sustainment activities necessary to maintain the ITSM tools configuration and enhancement Environment available to support system enhancement efforts.

2.1.5.4 The Contractor shall assess the hardware and software configuration of the ITSM tools configuration and enhancement Environment and conduct a capability comparison against the EITC production environment with respect to the configuration and enhancement of the environment's suitability and effectiveness as an environment for producing ITSM tool products for the EITC. The Contractor shall perform remediation tasks as necessary to ensure the ITSM tools configuration and enhancement Environment mirrors the production environment.

2.1.5.5 The Contractor shall maintain CfM including hardware, software, networking, and operational procedures for the tools configuration and enhancement environment.

2.1.5.6 The Contractor shall provide ITSM tools technical support to the Government EEVE lab manager in maintaining the ITSM tools configuration and enhancement environment so it is up and available to conduct ITSM tool enhancement and configuration.

2.1.5.7 The Contractor shall evaluate all changes to be applied to the ITSM toolset production environment within the ITSM tools configuration and enhancement Environment prior to submitting change proposals for production implementation.

2.1.5.8 The contractor shall acknowledge Advanced Technical Problems/Issues and respond to the related tickets within two (2) hours of verbal notification and/or ticket creation by MCNOSC. The response should come from a Contractor employee. The Contractor's relevant technical SME that has acknowledged the related incident/problem ticket must provide verbal or written notification to the Government operational POC. The contractor shall provide written updates (including summary of problem/issue or requirement, actions taken in the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion) to the Government operational POC until the problem/issue is resolved. These written updates shall be provided, at a minimum, for 95% of all such occurrences. Advanced Technical

Problems/Issues data shall be compiled in the weekly and monthly status reports

2.1.6 **Optional Objective 6: ITSM Tool Suite Enhancement**

The Marine Corps seeks support for enhancement of the ITSM tools suite. Some of the existing tools may require upgrades or enhancements during the PoP and additional supporting tools may require implementation to support ITSM process enhancement. New system enhancement projects may focus on one or more of the capabilities listed below and may span several of the process areas. The following optional CLINs describe new capabilities which may be exercised at the Government's discretion to design, enhance, configure, customize, test, implement, and document new ITSM capabilities that may be required to perform IT service management on behalf of the Marine Corps. These optional CLINs will be considered for award as Marine Corps ITSM environment matures over the period of performance. The timing of the option CLINs and placement within subsequent option years represents the Government's best estimates for when those services will be required.

2.1.6.1 **General Requirements for Objective 6**

The following activities shall be performed in addition to the specific optional objective tasks:

- The Contractor shall ensure that the ATO is retained through all Marine Corps ITSM upgrades and capability improvements.
- The Contractor shall document all changes and place them under USMC configuration management (CfM) utilizing the documentation and review requirements listed in Section 2.1.1.9. The Contractor shall use strict CfM for all hardware, software, documentation, and deliverables.
- The Contractor shall design, develop and maintain a New Equipment Training (NET) package. All training materials shall meet the training materials requirements listed in Section 2.1.3.
- The Contractor shall conduct NET prior to solution deployment.

2.1.6.2 **MEMS/Remedy Integration**

- The Contractor shall ensure that the Remedy system incorporates design features that enable the automated creation and assignment of a Remedy Incident record through integration with Marine Corps Event Management systems System (MEMS) based on authorized user definable event conditions.

2.1.6.3 **Remedy/Navy Enterprise Tool Integration**

The Contractor shall design, configure, enhance, document and implement a solution within the existing Remedy Request Fulfillment module to:

- Capture specific IT order requirements;
- Pass them to the Navy Enterprise Tool system for order processing;
- Log the order status within a Remedy Service Request record; and
- Track the external system activities to completion.

2.1.6.4 **Remedy/PR Builder Integration**

- The Contractor shall design, configure, enhance, document and implement a solution within the existing Remedy Request Fulfillment module to:
- Establish order procurement workflows;
- Capture financial information from Remedy requests to the USMC PR Builder system;
- Log the order status within a Remedy Service Request record; and
- Track the external system activities to completion.

2.1.6.5 **Remedy/ITPRAS Integration**

The Contractor shall design, configure, enhance, document, and implement a custom application within the existing Remedy solution to perform the following workflows to replace the current IT Procurement Request Approval System (ITPRAS):

- Allow users to submit requests to expend funds against IT hardware, software, and services;

- Route expenditure request based on funding type, funding amount, user's organization, request type (hardware, software, services) for multileveled approvals across multiple organizations;
- Log specific data attributes regarding each request submission (e.g. Summary, IT waivers, fiscal year requirements, funding type, etc.); and
- Track the progress of each request and report statuses to authorized users.

2.1.6.6 **Asset Discovery Integration**

The Contractor shall design, develop, document and implement asset discovery integration and normalization rules, processes and solutions to support MEMS discovery of servers and infrastructure assets. The solution shall provide auto-population of Remedy Atrium CIs with discovered data. The Contractor shall identify, implement and integrate additional Asset Scanning technologies with current E-ITSM tool suites. The solution shall enable telephone/bring-your-own-device (BYOD) discovery and CMDB population solutions.

2.1.6.7 **DML CI Establishment**

The Contractor shall design and implement an approach to integrate the USMC Definitive Media Library (DML) content into the CMDB as CIs:

- The Contractor shall enable the authorized user to visualize the set of DML solution entries as CIs according to lifecycle stages and associated IT services.
- The Contractor shall enable the authorized user to create, for a given DML solution, the relationships among the associated service entries, requests, and CI entries as part of the associated DML entry.

2.1.6.8 **Service Level Monitoring**

The Contractor shall enhance the existing ITSM Tool Suite to enable the authorized user to monitor customer usage and service usage for each service utilizing the existing MEMs solution.

2.1.6.9 **Remedy Enhanced Function**

The Contractor shall enhance existing ITSM tool suite through implementation of BMC MyIT functionality within the existing Remedy tool suite to enable self-service incident and knowledge management, social media, and service catalog access functionality utilizing location, role, and preferences to guide users to Remedy resources with formless requests, context-aware services, and crowd sourced collaboration.

2.1.6.10 **Continuity of Operations**

The Contractor shall design, configure, enhance, document, and implement ITSM tools suite failover and COOP solution within the MCEITS Failover Data Center currently expected to be located at Camp Lejeune in Jacksonville, NC for NIPRNet and SIPRNet production instances uPROD and cPROD respectively.

2.1.6.11 **Training Stack Migration**

The Contractor shall configure, enhance, and support implementation of a migration plan to re-locate the ITSM Tool Suite training environment from MCTSSA, Camp Pendleton, CA into the MCEITS Data Center hosting environment.

The Contractor shall identify, describe, and assist in implementation of the modifications or enhancements the training environment or MCEITS Data Center hosting environment requires, if any, to allow migration plan execution.

2.1.7 **Optional Objective 7: ITSM Training Activities**

The Marine Corps seeks support to develop training materials as gaps in the existing training solution set are identified. The following optional CLINs describe training materials which will require configuration, enhancement or training which will need to be conducted upon execution of the appropriate option.

2.1.7.1 **Enhancement of ITSM CBTs**

The Contractor shall configure a new CBT module or enhance an existing CBT module for a TBD new ITSM process, business process, or ITSM tool. The CBT is expected to be similar in complexity to the existing CBTs provided as GFI for the existing processes. The module shall include an assessment to measure a student's understanding of the module's content. The Contractor shall provide a draft storyboard for Government approval prior to CBT configuration or enhancement. The Contractor shall provide the code/editable version of the CBT. The Contractor shall assist the Government in configuration and enhancement of MarineNet hosting submission documentation and process. Training materials shall follow the MarineNet Courseware Configuration Technical Requirements for CBTs. Each shall be Shareable Content Object Reference Model (SCORM) Compliant and also have the ability to be hosted in a Learning Management System (LMS).

2.1.7.2 **Enhancement of ITSM JITs**

The Contractor shall configure a new JIT or enhance an existing JIT for a TBD new ITSM process, business process, or ITSM tool. The JIT is expected to be similar in complexity to the existing JITs provided as GFI for the existing processes. The Contractor shall provide a draft script for government approval prior to JIT configure, enhancement. If applicable, the Contractor shall provide the code/editable version of the JIT. Upon government acceptance, the Contractor shall load the JIT into Remedy Help for user access.

2.1.7.3 **Configuration and Enhancement of ITSM Job Aids**

The Contractor shall configure a new ITSM Job Aid or enhance an existing ITSM Job Aid for a TBD new ITSM process, business process, or ITSM tool. The Job Aid is expected to be similar in complexity to the existing Job Aids provided as GFI for the existing processes. The Contractor shall provide the sequenced draft script and screen shots for government approval prior to Job Aid configuration and enhancement. If applicable, the Contractor shall provide the editable version of the Job Aid. Upon government acceptance, the Contractor shall load the Job Aid into Remedy Help for user access.

2.1.7.4 Conduct Onsite Training for Existing ITSM Capabilities

The Contractor shall conduct onsite regional training overviewing existing USMC ITSM tool suite capabilities to an audience of approximately twenty-five (25) personnel and unlimited virtual attendance, not to exceed three (3) days per training event. Up to eight (8) training events will be conducted. Historically, one event was conducted per location. Historical locations have been at Quantico, VA; Washington, DC; Lejeune, NC, Pendleton, CA; New Orleans, LA; Okinawa, Japan; Kaneohe Bay, HA; Kansas City, MO; and Panser Kaserne, Germany.

3.0 Government Furnished Equipment (GFE) and Government Furnished Information (GFI)

3.1 Information

The documents listed below in Table 1, will be made available via the Safe Access File Exchange tool, which can be found at https://safe.amrdec.army.mil/safe/. To receive the documents, Contractors should respond to the POC listed in the RFP and provide a Contractor POC name, email address, and phone number. Access information will be sent to the Contractor POC. If any additional documents become necessary, please send a request to the contract specialist listed in the solicitation and the same will be shared if deemed necessary.

Table 1. GFI Documents

Item	Qty
MCIENT Strategy	1
MCIE SE COE	1
MCEN Unification Plan	1
Marine Corps Message 021815Z Jul 2008	1
Marine Corps Message 021903Z Jul 2008	1
Marine Corps Systems Command Order 4130.1	1
Marine Corps Systems Command Technical Review Handbook v1.04	1
DoD NetOps Strategic Vision	1
Global Information Grid (GIG) NETOPS Concept of Operations (CONOPS)	1
NetOps for the GIG	1

Marine Corps ITSM Process Guides (IM, EM, ChM, SACM, SCM, RDM, RqF, PM, KM and SLM, IdAM, DM, CpM, AvM)	14
USMC TDLC documentation	1
Marine Corps ITSM TDPs	1
Marine Corps ITSM P/WIs	1
Marine Corps ITSM FDDs	1
Marine Corps ITSM Training Documentation	1
IS&I Engineering Document Templates	9

3.2 Government-Furnished Property/Equipment (GFP/GFE)

The Government will provide desk space in the EV Lab. However, Government owned computer equipment and phones will not be provided.

To support the establishment and sustainment of ITSM tools associated with this task, the Government will provide the following software items for use in ITSM tools configuration, enhancement, and test activities:

- BMC Remedy
- HP uCMDB
- HP uCMDB Probes
- Kelverion Windows Orchestrator
- SCCM 2012
- Windows Server
- Active Directory
- RedHat Linux
- MSSQL, Oracle
- CAC Single Sign On

The Contractor shall provide any additional configuration and enhancement tools identified as required within their Technical Approach.

4.0 Contractor Furnished Items and Responsibilities

4.1 General

The Contractor shall furnish all supplies, computer equipment, facilities, and services that are not listed under Section 3.2 required to perform work under this PWS.

Hardware/Software Requirements: The contractor shall arrive on site with all equipment necessary to fully perform the tasks identified within this performance work statement (e.g. cell phones, including OCONUS access; end user devices with appropriate software and internet connectivity (e.g. CAC enabled workstations with air cards, etc.); and tools and test equipment (e.g. screwdrivers, pliers, voltmeters, time domain reflectometers, cable tipping kits, cable testers, etc.)). In addition, contractors shall have:

- System Account Authorization Requests (SAARs) processed and MCEN account access.
- Each contractor employee's JPAS record must also reflect a favorably adjudicated personnel security Investigation (PSI)).
- Mobile phones for the contractors traveling OCONUS that shall support International use.
- Laptops must have sufficient screen resolution and video processing to support viewing multiple large documents in support of installation.
- At a minimum, the laptop specifications should include (at least):
    - 1 GB Ethernet Port
    - Available DVD-DL +r /-r drive
    - Available USB 2.0 or higher ports
    - Serial Port or available USB to Serial Port adapter
    - Compatible with Windows 7 and Windows 10
    - CAC-enabled
    - MS Visio 2010 Professional installed
    - MS Office 2010 or later, installed
    - Secure Shell Software
    - Wireless network adapters must be disabled in BIOS

The Contractor shall be responsible for all local travel expenses necessary for their personnel to perform the required services as defined in section 1.4.3 related to travel ODCs.

4.2 Security Requirements

This contract will require the Contractor to have a valid Secret Facility Clearance and will require certain

contractors to obtain and maintain classified access eligibility. The contractor shall have a valid Secret Facility Clearance prior to classified performance. The prime contractor and all sub-contractors (through the prime contractor) shall adhere to all aspects of DoD Directive 5220.22-M. All personnel identified to perform on this contract shall maintain compliance with Department of Defense, Department of the Navy, and Marine Corps Information and Personnel Security Policy to include completed background investigations (as required) prior to classified performance. Classified access is required in order to attend meetings and perform daily work inside approved areas. Access entails unescorted access into classified spaces and access to classified information and/or systems (SIPRNET). There will be classified products created, used, and stored under this contract.

This contract shall include a DoD Contract Security Classification Specification (DD Form 254) as an attachment. Requests for Contractor SIPRNet accounts will be handled on a case-by-case basis and approved individually by the COR in accordance with Marine Corps Systems Command procedures and regulations. The Contractor shall notify the Government (written notice) within twenty-four hours of any Contractor personnel added or removed from the contract that have been granted classified access, issued a Common Access Card and/or MARCORSYSCOM Building access.

The Contractor shall be responsible for safeguarding all Government equipment, information, and property provided for Contractor use. The prime Contractor and all sub-Contractors (through the prime Contractor) shall certify in writing to the Government that personnel supporting this contract are “Qualified U.S. Contractors” per DoD Directive 5220.22-M, Chapter 2, Section 2. Qualified U.S. Contractors are restricted to U.S. citizens, persons admitted lawfully into the United States. The Government shall assist the Contractor in gaining access to Government agencies and installations related to the systems in question. The Contractor shall ensure that the employees are on the approved Government access list prior to entering any access controlled area. The Contractor shall notify the Government (written notice) within 24 hours of Contractor personnel added or removed from the access control list.

4.3 Common Access Card (CAC) Requirement

The COR will identify and approve those contractor employees performing on this contract that require Common Access Cards (CACs) in order to perform their job function. In accordance with Headquarters, United States Marine Corps issued guidance relative to Homeland Security Presidential Directive – 12 (HSPD-12), all personnel must meet eligibility criteria to be issued a CAC. In order to meet the eligibility criteria, contractor employees requiring a CAC, must obtain and maintain a favorably adjudicated Personnel Security Investigation (PSI). Prior to authorizing a CAC, the employee's JPAS record must indicate a completed and favorably adjudicated PSI or (at a minimum) that a PSI has been submitted and accepted (opened). The minimum acceptable investigation is a National Agency Check with Written Inquiries (NACI.) If a contractor employee's open investigation closes and is not favorably adjudicated, the CAC must be immediately retrieved and revoked.

Facility Security Officers (FSOs) are responsible for notifying the MCSC Security Director if any contractor performing on this contract receives an unfavorable adjudication after being issued a CAC. The FSO must also notify the MCSC Security Director of any adverse/derogatory information associated with the 13 Adjudicative Guidelines/Factors concerning any contractor issued a CAC, regardless of whether a JPAS Incident Report is submitted.

Each CAC is issued with a "ctr.usmc.mil" e-mail account that the individual contractor is responsible to keep active by logging in on a regular basis (at least twice a month), sending an e-mail and clearing any unneeded e-mails. Contractors are prohibited from "auto-forwarding" their .mil e-mail account to their .com e-mail account. If the ctr.usmc.mil e-mail account is not kept active, the G-6 will deactivate the account and CAC will lose its functionality.

CACs will only be issued to those contractors supporting this contract that have been authorized by the COR. The COR will only authorize CACs for those contractors that meet current HSPD-12 criteria and have a definitive requirement.

If a contractor loses their eligibility for a CAC due to an adverse adjudicative decision, they have also lost their eligibility to perform on MCSC contracts. CACs are not issued for convenience.

4.4 Certification and Accreditation (C&A)

The Contractor shall mitigate all issues that may impact the security and accreditation of the Marine Corps ITSM systems. The Contractor shall provide security requirement identification analysis, allocation, and tracking support as specified utilizing DoD RMF documentation as required and comply with IA guidelines.

4.5 ITSM tools Configuration, Enhancement and Testing Environments

The Contractor shall provide any software beyond that listed in Section 1.2.2 deemed necessary by the Contractor to perform solution design, configuration, and enhancement activities including but not limited to application and training material configuration and enhancement.

5.0 Definitions

5.1 Deliverables

A deliverable list of authorized data requirements for a specific procurement that forms a part of the contract is located in Appendix B. The deliverable list specifies the data to be produced by the Contractor and when it is to be delivered.

5.2 Contracting Officer (KO)

A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the Government. Note: The KO is the only individual who can legally bind the Government.

5.3 Contracting Officer's Representative (COR)

A Contracting Officer Representative will be appointed by the Contracting Officer to assist in the administration of the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

5.4 Quality Assurance (QA)

The processes and procedures used to monitor, detect, correct, and verify that services are performed according to acceptable standards.

5.5 Quality Assurance Program Plan (QAPP)

The Contractor developed QAPP describes how the Contractor will conduct Contractor performance reporting to ensure systematic quality assurance methods are being used to validate that the Contractor's quality control efforts are timely, effective, and are delivering the results specified in the Marine Corps ITSM contract. The QAPP directly corresponds to the performance objectives and standards specified in this PWS and the Government QASP.

5.6 Quality Control (QC)

All necessary measures taken by the Contractor to assure that the quality of a product or service shall meet contract requirements.

6.0 Applicable Publications (Current Editions)

The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures. The Marine Corps ITSM documents listed in Table 1 provide essential programmatic information that needs to be considered in the Contractor’s initial proposal.

In addition, the Contractor is required to perform in compliance with the most recent version of the following requirements, standards, and guidelines:

6.1 Compliance Documents

The following documents or references are applicable to this PWS to the extent specified herein:

- National Industrial Security Program Operating Manual (NISPOM – DoD Directive 5220.22-M)
- DFARS 252.232-7003
- DFARS 252.211-7003
- FAR 9.5
- MIL-HDBK-61A
- DoD Directive 5000.01, The Defense Acquisition System
- Functional Design Documents (to be provided as GFI)
- DoD 8750 series of instructions

6.2 Security Related Guidance

- Federal Information Security Management Act (FISMA) of 2002
- DoDD 8500.01E, Information Assurance (IA), 24 Oct 2002 (current as of 23 Apr 2007)
- DoDI 8500.2, Information Assurance (IA) Implementation, 6 Feb 2003
- DoD 8570.01M, Information Assurance Workforce Improvement

Program, Incorporating Change3, January 24, 2012

- CJCSI 6510.01F, Information Assurance and Computer Network Defense, 09 February 2011
- SECNAVINST 5000.2E, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, 01 September 2011
- DoD 5200.2-R, Personnel Security Program
- DoDD 8000.01, Management of the DoD Information Enterprise
- NFPA 75 (Standard for the Protection of Information Technology Equipment)
- MCO 5239.1, Marine Corps Information Assurance Program (MCIAP)
- MCO 5239.2A Marine Corps Cyber Security Program (MCCSP), 18 July 2012
- MARADMIN 257/12 UPDATES TO ANNUAL CYBER AWARENESS TRAINING
- MARADMIN 639/08, MCBUL 5239 USMC IA VULNERABILITY MANAGEMENT (IAVM) PROGRAM
- IETF RFC 4346 - The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006.
- The Certificate Issuing and Management Components (CIMC) Family of Protection Profiles (PPs), Ver 1.5 11 August 2011 (http://www.commoncriteriaportal.org/pp_OD.html)
- WARP Ports and Protocol Description
- SIAT RMF Process Guidance document (draft)

6.3 Standards

- MIL-PRF-49506 (Performance Specification - Logistics Management Information); November 1996
- MIL-HDBK-470A (Designing and Developing Maintainable Products and Systems, Vol 1); 04 December 1997
- MIL-HDBK-781A (Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production); April 1996
- ASME Y14.34-2008 (Associated Lists)
- ASME Y14.100-2004 (Reaffirmed 2009) (Engineering Drawing Practices)
- ASTM F1166-07 (Standard Practice for Human Engineering Design for Marine Systems, Equipment, and Facilities)
- EIA-625 (Requirements for Handling Electrostatic Discharge-Sensitive (ESDS) Device)
- EIA-649-A, April 2004 (National Consensus Standard for Configuration Management)
- Capabilities Maturity Model Integration (CMMI) v1.3, November 2010.

6.4 Other Guidance

- DoD 5000.02, Operation of the Defense Acquisition System, 02 December 2008
- Defense Acquisition Guidebook (https://dag.dau.mil/Pages/Default.aspx)
- DoD 8500 series of instructions
- DoDI 8510.01
- MCSC Order 4130.1, Configuration Management Policy
- MCSC Order 5000.3 Naval SYSCOM Risk Management Policy
- IEEE/EIA 12207.0-1996, IEE Standard for Information Technology- Software Life Cycle Processes
- ISO/IEC 15289:2011, Systems and software engineering – Content of life cycle process information products (documentation)
- DFARS 252.211-7003and MIL-STD-130N, Item Identification and Valuation contractual requirements for IUID
- DoD Guide to Uniquely Identifying Items, Ver.2.5, 15 Sept 2012 (replaces all previous versions)
- DISA Policy and Guidance (http://iase.disa.mil/policy-guidance/index.html)
- ASN(RD&A)Guidebook for Acquisition of Naval Software Intensive Systems, Ver 1.0, September 2008; (http://acquisition.navy.mil/rda/content/view/full/6079
- MARCORSYSCOM Acquisition Guidebook (MAG), V1.0, March 2012
- Marine Corps Systems Command Technical Review Handbook V1.04, April 2009
- DoD Joint Travel Regulations
- Department of Defense Architecture Framework Version 2.0

7.0 Acronyms

ACL	Access Control List
ATO	Authority to Operate
B/P/S	Base/Post/Station
BYOD	Bring Your Own Device
C&A	Certification and Accreditation
CAB	Change Advisory Board
CAE	Client Automation Enterprise
CBT	Computer Based Training
CDR	Critical Design Review

CDRL	Contract Data Requirements List
cEITC	Classified Enterprise Information Technology Center
CfM	Configuration Management
ChM	Change Management
CI	Configuration Item
CITDB	Configuration Item Technical Data Base
CMDB	Configuration Management Database
CMP	Configuration Management Plan
CMS	Configuration Management System
COE	Concept of Employment
COR	Contracting Officer Representative
CPR	Critical Process Review
cPROD	Production environment on the secure network
CRM	Comment Resolution Matrix
CSI	Continual Service Improvement
CVS	Contractor Verification System
WBS	Work Breakdown Structure
DBA	Database Administrator
DD254	Department of Defense Contract Security Requirement List
DDS-M	Data Distribution System – Modular
DFARS	Defense Federal Acquisition Regulation Supplement
DITIL	Defense Information Technology Infrastructure Library
DoD	Department of Defense
DoDI	Department of Defense Instruction
DON	Department of the Navy
EITC	Enterprise Information Technology Center
EM	Event Management
ESD	Enterprise Service Desk
FAR	Federal Acquisition Regulation
FDD	Functional Design Document
FISMA	Federal Information Security Management Act

FTE	Full-Time Equivalents
FY	Fiscal Year
GAT	Government Acceptance Test
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GIG	Global Information Grid
GOGO	Government-Owned, Government-Operated
GPO	Government Printing Offices
HP	Hewlett Packard
HPES	Hewlett Packard Enterprise Services
HPNA	HP Network Automation
HPSA	HP Server Automation
HQMC C4	Headquarters Marine Corps Command, Control, Communications, and Computers
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
IM	Incident Management
IMS	Integrated Master Schedule
IPT	Integrated Product Team
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITPRAS	Information Technology Procurement Request Review/Approval System
ITSM	Information Technology Service Management
JIT	Just in Time Videos
JPAS	Joint Personnel Adjudication System
KM	Knowledge Management
KO	Contracting Officer
LMS	Learning Management System
LMST	Lightweight Multiband Satellite Terminal
MAC	Mission Assurance Category
MARCORSYSCOM	Marine Corps Systems Command

MARFOR	Marine Forces
MCCAP	Marine Corps Certification and Accreditation Process
MCCAST	Marine Corps Certification & Accreditation Support Tool
MCEIAD	Marine Corps Enterprise Information Assurance Directive
MCEITS	Marine Corps Enterprise Information Technology Services
MCEN	Marine Corps Enterprise Network
MCI	Marine Corps Installation
MCIE	Marine Corps Information Environment
MCIENT	Marine Corps Information Enterprise
MCITE	Marine Corps Information Technology Environment
MCNIS	Marine Corps Network and Infrastructure Services
MCNOSC	Marine Corps Network Operations and Security Command
MCSC	Marine Corps Systems Command
MCTSSA	Marine Corps Tactical Systems Support Activity
MEMS	Marine Corps Event Management System
MEP	Most Essential Process
MITSC	Marine Air-Ground Task Force (MAGTF) Information Technology Support Center
MS	Microsoft
MSR	Monthly Status Report
NET	New Equipment Training
NetOps	Network Operations
NetCOP	Network Common Operational Picture
NIPRNet	Non-classified Internet Protocol Router Network
NGEN	Next Generation Enterprise Network
NLT	No Later Than
NNMi	Network Node Manager interface
ODC	Other Direct Costs
OLA	Operating Level Agreement
OpDir	Operational Directive

O&S	Operations and Sustainment
OSI	Open Systems Interconnection
PbM	Problem Management
PD2	Procurement Desktop 2
PDR	Preliminary Design Review
POA&M	Program of Action & Milestone
PoP	Period of Performance
POR	Program of Record
PPR	Preliminary Process Review
P/WI	Procedures/Work Instructions
PWS	Performance Work Statement
QA	Quality Assurance
QAPP	Quality Assurance Program Plan
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
RASCI	Responsible, Accountable, Supportive, Consulted, & Informed
RDM	Release and Deployment Management
RFC	Request for Change
RNOSC	Regional Network Operations and Security Center
ROM	Rough Order of Magnitude
RPO	Recovery Point Objective
RqF	Request Fulfillment
RTO	Recovery Time Objective
SLA	Service Level Agreement
SA	Situational Awareness
SAAR	System Account Access Request
SACM	Service Asset and Configuration Management
SAT	Systems Approach to Training
SCCM	System Center Configuration Manager
SCM	Service Catalog Management
SCORM	Shareable Content Object Reference Model

SE	Systems Engineering
SECNAVINST	Secretary of the Navy Instruction
SETR	Systems Engineering Technical Review
SIE	Systems Integration Environment
SLM	Service Level Management
SLT	Service Level Target
SPM	Service Portfolio Management
SRM	Service Request Management
SVR	System Verification Review
SWAN	Support Wide Area Network
TAR	Tool Access Request
TcSE	Teamcenter Systems Engineering
TDLC	Technical Delivery Life Cycle
TDP	Technical Data Package
TSST	Phoenix Tactical SHF Satellite Terminal
UC	Underpinning Contracts
uCMDB/DDMa	Universal Configuration Management Database/Dependency Mapping Advanced Edition
uEITC	Unclassified Enterprise Information Technology Center
uPROD	Production environment on the non-secure network
USMC	United States Marine Corps

Appendix A - Performance Requirements Summary

PWS Paragraph	Task	Performance Standard	Acceptable Quality Levels (AQL)	Surveillance Method / By Whom
2.1.1.1 Objective 1: Program Management	The contractor shall submit initial IMS, WBS, RMP, PMP, and staffing plan as Deliverables within the established timeframe.	The contractor shall submit initial IMS, WBS, RMP, PMP, and staffing plan IAW the deliverables timeframe as stated in Appendix B – Program Deliverables of the PWS, 100% of the time.	0% failure to submit initial IMS, WBS, RMP, PMP, staffing plan as Deliverables within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated in PWS Appendix B – Program Deliverables
2.1.1.2 Objective 1: Program Management	The contractor shall submit updated IMS within the established timeframe.	The contractor shall submit updated IMS IAW the deliverable timeframe as stated in Appendix B – Program Deliverables of the PWS, 100% of the time.	0% failure to submit updated IMS IAW the deliverable within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated in PWS Appendix B – Program Deliverables
2.1.1.3 Objective 1: Program Management	The contractor shall submit updated WBS, Staffing Plan within the established timeframe.	The contractor shall submit updated WBS, Staffing Plan IAW the deliverable timeframe as stated in Appendix B – Program	0% failure to submit updated WBS, Staffing Plan IAW the deliverable within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated in PWS Appendix B – Program

		Deliverables of the PWS, 100% of the time.		Deliverables
2.1.1.4 Objective 1: Program Management	The contractor shall submit updated RMP within the established timeframe.	The contractor shall submit updated RMP IAW the deliverable timeframe as stated in Appendix B – Program Deliverables of the PWS, 100% of the time.	0% failure to submit updated RMP IAW the deliverable within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated in PWS Appendix B – Program Deliverables
2.1.1.5 Objective 1: Program Management	The contractor shall submit weekly status reports within the established timeframe.	The contractor shall submit weekly status reports IAW the deliverable timeframe as stated in Appendix B – Project Deliverables of the PWS, 99% of the time.	1% failure to submit weekly status reports IAW the deliverable within the established timeframe.	100% Inspection – COR shall be in receipt of the deliverable NLT the submission timeframe stated in PWS Appendix B –Program Deliverables
2.1.1.6 Objective 1: Program Management	The contractor shall deliver fully functional and effective ad-hoc meeting support and reporting within the established timeframe.	The contractor shall deliver fully functional and effective ad-hoc meeting support and reporting IAW the deliverable timeframe as stated in Appendix B – Program Deliverables of the PWS, 99% of the time	1% failure to deliver fully functional and effective ad-hoc meeting support and reporting IAW the deliverable within the established timeframe.	Periodic Inspection by the COR on a quarterly basis.
2.1.1.9 Objective 1:	The contractor shall provide Engineering	The contractor shall provide Engineering	0% failure to provide Engineering	100% Inspection – COR will review

Program Management	Design/Documentation (DEVDOCS) within the established timeframe.	Design/Documentation within the established timeframe 100% of the time.	Design/Documentation within the established timeframe.	Engineering Design/Documentation on a quarterly basis.
2.1.1.9 Objective 1: Program Management	The contractor shall support successful completion of SETR events within the established timeframe	The contractor shall support successful completion of SETR events within the established timeframe 100% of the time.	0% failure to support successful completion of SETR events within the established timeframe.	100% Inspection – COR will review Presentation Materials and Meeting Minutes, Functional Design Documents, Test Plan on a quarterly basis.
2.1.1.9 Objective 1: Program Management	The contractor shall submit DoD Risk Management Framework Documentation in support of IA within the established timeframe.	The contractor shall submit DoD Risk Management Framework Documentation in support of IA within the established timeframe 100% of the time.	0% failure to submit DoD Risk Management Framework Documentation in support of IA within the established timeframe.	100% Inspection – COR will continuously monitor IA documentation on a quarterly basis.
2.1.1.9 Objective 1: Program Management	The contractor shall submit documents for USMC review IAW Technical Review Action Plan (TRAP) within the established timeframe.	The contractor shall submit documents for USMC review IAW Technical Review Action Plan (TRAP) within the established timeframe 100% of the time.	0% failure to submit documents for USMC review IAW Technical Review Action Plan (TRAP) within the established timeframe.	100% Inspection – COR will review Presentation Materials and Meeting Minutes, Functional Design Documents, Test Plan on a quarterly basis.
2.1.1.11, 2.1.1.12	The contractor shall administer a quality	The contractor shall administer a quality	failure to administer a quality	Periodic Inspection by the COR on a

Objective 1: Program Management	control plan including sub-contractor management IAW the deliverable QAPP within the established timeframe.	control plan including sub-contractor management IAW the deliverable QAPP within the established timeframe 95% of the time.	control plan including sub-contractor management IAW the deliverable QAPP within the established timeframe.	quarterly basis.
2.1.2.2 Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall perform restorative maintenance within the established timeframes.	The contractor shall perform restorative maintenance within the established timeframes 98% of the time each month.	2% failure to perform restorative maintenance within the established timeframes each month.	Periodic Inspection - COR will review monthly work order logs.
2.1.2.2 Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall acknowledge tickets after verbal notification and ticket creation by MCNOSC related to problems and issues within the established timeframe.	The contractor shall acknowledge tickets after verbal notification and ticket creation by MCNOSC related to problems and issues within the established timeframe 95% of the time.	5% failure to acknowledge tickets after verbal notification and ticket creation by MCNOSC related to problems and issues within the established timeframe.	Periodic Inspection – The COR will inspect contractor weekly status reports and monthly status reports on a quarterly basis.
2.1.2.2 Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall provide written updates to the Government operational POC when advanced technical problems/issues are resolved within the established	The contractor shall provide written updates to the Government operational POC when advanced technical problems/issues are resolved within the established	5% failure to provide written updates to the Government operational POC when advanced technical problems/issues are resolved within the established	Periodic Inspection – The COR will inspect contractor weekly status reports and monthly status reports on a quarterly basis.

	timeframe.	timeframe 95% of the time.	timeframe.	
2.1.2.2 Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes.	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes 98% of the time.	2% failure to restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.1.2.2 Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall maintain ITSM toolset availability (based on contractor caused unplanned downtime) within the established timeframe.	The contractor shall maintain ITSM toolset availability (based on contractor caused unplanned downtime) within the established timeframe 98% of the time.	2% failure to maintain ITSM toolset availability (based on contractor caused unplanned downtime) within the established timeframe.	Periodic Inspection – The COR will inspect contractor weekly status reports and monthly status reports on a quarterly basis.
2.1.2.2 Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall restore ITSM tools classified under RMF as Medium-Medium-Low within the established timeframe.	The contractor shall restore ITSM tools classified under RMF as Medium-Medium-Low within the established timeframe 98% of the time.	2% failure to restore ITSM tools classified under RMF as Medium-Medium-Low within the established timeframe.	Periodic Inspection – The COR will inspect contractor weekly status reports and monthly status reports on a quarterly basis.
2.1.2.2 Objective 2: ITSM Tool Suite Operations &	The contractor shall deliver fully functional and effective ad-hoc reporting within the established	The contractor shall deliver fully functional and effective ad-hoc reporting within the established	5% failure to deliver fully functional and effective ad-hoc reporting within the established	Periodic Inspection – The COR will inspect Ad-Hoc Reports on a quarterly basis.

Maintenance	timeframe.	timeframe 95% of the time. Ad-hoc report turnaround shall be within 5 working days.	timeframe.	
2.1.2.1, 4.2.2 Objective 2: ITSM Tool Suite Configuration & Enhancement	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within the established timeframe.	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within the established timeframe 95% of the time. All RMF packages shall be at least 90% correct, requiring no greater than 10% rework.	5% failure to submit DoD RMF packages, which are at a minimum 90% correct, requiring no greater than 10% rework, when required due to system changes or security requirements within the established timeframe.	Periodic Inspection – The COR will inspect IA artifacts on a quarterly basis.
2.1.2.1, 4.2.2, Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within the established timeframes.	The contractor shall submit DoD RMF packages when required due to system changes or security requirements within the established timeframes 95% of the time.	5% failure to submit DoD RMF packages when required due to system changes or security requirements within the established timeframes.	Periodic Inspection – The COR will inspect IA artifacts on a quarterly basis.
2.1.2.1, 2.1.2.1, 4.2.2 Objective 2: ITSM Tool Suite	The contractor shall apply all required security patches or updates as required and remediate any ITSM system	The contractor shall apply all required security patches or updates as required and remediate any ITSM system	5% failure to apply all required security patches or updates as required and remediate any ITSM system	Periodic Inspection – The COR will inspect IA artifacts on a quarterly basis.

Operations & Maintenance	functionality affected by such updates within the established timeframes.	functionality affected by such updates within the established timeframes 95% of the time. Security patches applied within one week of Information Assurance Vulnerability Alert (IAVA) release notice or based on USMC direction.	functionality affected by such updates within the established timeframes.	
2.1.2.1, 2.1.2.3 2.1.6.1, Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall Ensure that the ATO remains in effect at all times during the PoP within the established timeframes.	The contractor shall Ensure that the ATO remains in effect at all times during the PoP within the established timeframe. 100 % system compliance with RMF, the FISMA, and the Marine Corps Enterprise Information Assurance Directive (MCEIAD).	0% failure to Ensure that the ATO remains in effect at all times during the PoP.	100% Inspection – COR will review IA Artifacts and compliance with the PWS.
2.1.2.1, Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall provide the required SCAN reports and Program of Action & Milestones (POA&Ms) to demonstrate the changes have been	The contractor shall provide required SCAN reports and POA&Ms within the established timeframes 100% of	0% failure to provide required SCAN reports and POA&Ms within the established timeframes.	100% Inspection – COR will review IA Artifacts and compliance with the PWS.

	implemented correctly within the established timeframes.	the time.		
2.1.2.5 Objective 2: ITSM Tool Suite Operations & Maintenance	The contractor shall provide ITSM tools functionally capable according to the FDDs for implemented processes within the established timeframes.	The contractor shall provide ITSM tools functionally capable according to the FDDs for implemented processes within the established timeframes 100% of the time.	0% failure to provide ITSM tools functionally capable according to the FDDs for implemented processes within the established timeframes.	100% Inspection – COR will review IMS, WBS and compliance with the PWS.
2.1.3, 2.1.3.1, 2.1.3.2, 2.1.3.3, 2.1.3.4 Objective 3: Enhancement of ITSM Training Materials	The contractor shall provide accurate and complete training material within the established AQL.	The contractor shall provide accurate and complete training material and ensure the training material is in compliance with the planned syllabus and lesson plans within the established AQL 100% of the time.	0% failure to provide accurate and complete training material in compliance with the syllabus and lesson plans within the established AQL.	100% Inspection – COR will review training materials.
2.1.3, 2.1.3.1, 2.1.3.2, 2.1.3.3, 2.1.3.4 Objective 3: Enhancement of ITSM Training Materials	The contractor shall provide training material in compliance with Marine Corps SAT Manual and SCORM within the established AQL.	The contractor shall provide training material in compliance with Marine Corps SAT Manual and SCORM within the established AQL 100% of the time.	0% failure to provide training material in compliance with Marine Corps SAT Manual and SCORM within the established AQL.	100% Inspection – COR will review training materials.
2.1.4.4	The contractor shall	The contractor shall	5% failure to	Periodic Inspection

Objective 4: ITSM Toolset Training Environment	resolve advanced technical problems/issues in response to tickets received from MCNOSC or a verbal or written notification within the established timeframe.	resolve advanced technical problems/issues in response to tickets received from MCNOSC or a verbal or written notification within the established timeframe 95% of the time.	resolve advanced technical problems/issues in response to tickets received from MCNOSC or a verbal or written notification within the established timeframe.	– COR will review weekly status report, monthly status report on a quarterly basis.
2.1.4.4 Objective 4: ITSM Toolset Training Environment	The contractor shall provide written updates and summary to the Government operational POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours and estimated date/time of completion within the established timeframes.	The contractor shall provide written updates and summary to the Government operational POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion within the established timeframes 95% of the time.	5% failure to provide written updates and summary to the Government operational POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.1.4.4 Objective 4: ITSM Toolset Training Environment	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes 98% of	2% failure to restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.

	timeframes.	the time.	timeframes.	
2.1.5.4 Objective 5: ITSM Toolset Configuration &Enhancement Environment	The contractor shall acknowledge and respond to problem tickets within the established timeframes.	The contractor shall acknowledge and respond to problem tickets within the established timeframes 95% of the time.	5% failure to acknowledge and respond to problem tickets within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.1.5.4 Objective 5: ITSM Toolset Configuration &Enhancement Environment	The contractor shall provide written updates and summary to the Government operational POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours and estimated date/time of completion until the problem is resolved within the established timeframes.	The contractor shall provide written updates and summary to the Government operational POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours and estimated date/time of completion until the problem is resolved within the established timeframes 95% of the time.	5% failure to provide written updates and summary to the Government operational POC of problems/issues or actions taken within the last 24 hours, actions planned for the next 24 hours, and estimated date/time of completion until the problem is resolved within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.1.5.4 Objective 5: ITSM Toolset Configuration &Enhancement Environment	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes.	The contractor shall restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes 98% of	2% failure to restore ITSM tools and related infrastructure (e.g., databases, operating systems) within the established timeframes.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.

		the time.		
2.1.6 2.1.6.1 - 2.1.6.12 Optional Objective 6: ITSM Tool Suite Enhancement	The contractor shall provide high quality releases based on the Release Impact Rate as defined, where impact is the percentage of incidents per a given release.	The contractor shall provide high quality releases based on the Release Impact Rate Calculation of not more than 15%.	Not more than 15% of production releases in an annual period cause an incident.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.1.6, 2.1.6.1 - 2.1.6.12 Optional Objective 6: ITSM Tool Suite Enhancement	The contractor shall calculate the release rollback rate percentage as defined where a release must be rolled back to a prior state.	The contractor shall provide high quality releases based on the Release Rollback Rate Calculation of not more than 10%.	Not more than 10% of production releases in an annual period must be rolled back to a prior state.	Periodic Inspection – COR will review weekly status report, monthly status report on a quarterly basis.
2.1.6.11 Optional Objective 6: ITSM Tool Suite Enhancement	The contractor shall develop and support implementation of a migration plan to re-locate the ITSM Tool Suite training environment within the established timeframes.	The contractor shall develop and support implementation of a migration plan to re-locate the ITSM Tool Suite training environment within the established timeframes 100% of the time.	0% failure to develop and support implementation of a migration plan to re-locate the ITSM Tool Suite training environment within the established timeframes.	100% Inspection – COR will inspect the Migration Plan
2.1.7.1 - 2.1.7.4 Objective 7: Optional ITSM Training Activities	The contractor shall provide accurate and complete training material within the established AQL.	The contractor shall provide accurate and complete training material and ensure the training material is in	0% failure to provide accurate and complete training material in compliance with the syllabus and lesson	100% Inspection – COR will review training materials.

		compliance with the planned syllabus and lesson plans within the established AQL 100% of the time.	plans within the established AQL.	
2.1.7.1 - 2.1.7.4 Objective 7: Optional ITSM Training Activities	The contractor shall provide training material in compliance with Marine Corps SAT Manual and SCORM within the established AQL.	The contractor shall provide training material in compliance with Marine Corps SAT Manual and SCORM within the established AQL 100% of the time.	0% failure to provide training material in compliance with Marine Corps SAT Manual and SCORM within the established AQL.	100% Inspection – COR will review training materials.
2.1.7.1 - 2.1.7.4 Objective 7: Optional ITSM Training Activities	The contractor shall provide onsite training in compliance with the Contractor provided, Government approved training plan.	The contractor shall provide onsite training in compliance with the Contractor provided, Government approved training plan 100% of the time.	0% failure to provide onsite training in compliance with the Contractor provided, Government approved training plan.	100% Inspection – COR will monitor the training delivery

Appendix B –Program Deliverables

PWS Objectives #	PWS Section	Deliverable Title	Format	Date of first submission	Subsequent Submission
1	2.1.1.1, 2.1.1.2	Integrated Master Schedule (IMS)	MS Project DI-MGMT-81650	Draft at initial Government kick off meeting ;10 working days after Government kickoff meeting	NLT 15th of each month for previous month
1	2.1.1.1, 2.1.1.3	Work Breakdown Structure (WBS)	DI-MGMT-81334D	Draft at initial Government kick off meeting; 20 working days after Government kickoff meeting	NLT 15th of each month for previous month
1	2.1.1.1	Program Management Plan (PMP)	Contractor recommended DI-MGMT-81797	Draft at initial Government kick off meeting; final 30 working days after Government kickoff meeting	Annually if changes have occurred

PWS Objectives #	PWS Section	Deliverable Title	Format	Date of first submission	Subsequent Submission
1	2.1.1.6	Presentation Materials and Meeting Minutes	DI-ADMN-81505	NLT 5 days after the technical reviews/or any meetings have occurred	N/A
1	2.1.1.1, 2.1.1.3	Staffing Plan	Government approved Contractor Format	Draft at initial Government kick off meeting; 20 working days after Government kickoff meeting	NLT 15th of each month for previous month
1	2.1.1.5	Weekly Status Report	Government approved Contractor Format	1st week after contract award	NLT Thursday of each week
1, 2	2.1.1.7	Monthly Status Report	Government approved Contractor Format (to include Performance Metrics and Risks)	NLT 15th of each month for previous month	NLT 15th of each month for previous month
1	2.1.1.10, 2.1.1.11	Quality Assurance Program Plan (QAPP)	DI-QCIC-81794	1st Draft due with response to RFQ	Final Draft Due 10 days after contract award and annually if changes have occurred
1	2.1.1.1, 2.1.1.4	Risk Management Plan (RMP)	DI-MGMT-81808	Draft at initial Government kick off meeting; NLT 30 days after contract award	5 days after receipt of Government Comments Annually if changes have occurred

PWS Objectives #	PWS Section	Deliverable Title	Format	Date of first submission	Subsequent Submission
2,3,5,6	2.1.1.9, 2.1.2.3 2.1.6	Test Documentation (e.g., List of RFCs ready for release, Use Cases, Standard Test Process for Monthly Releases)	Government approved Contractor Format	NLT 30 days prior to test	5 days after receipt of Government Comments
2,3,5,6	2.1.2.1, 2.1.6, 4.2.2	IA Artifacts in compliance with PWS references	Government approved Contractor Format	As required	As required
2,3,5,6	2.1.2.1, 2.1.6, 4.2.2	Draft C&A Documentation	Government approved Contractor Format	120 days after award	N/A
2,3,5,6	2.1.2.1, 2.1.6, 4.2.2	Final C&A Documentation	Government approved Contractor Format	10 days after Government provides comments	N/A
2,3,4,5,6	1.4.5, 2.1.3, 2.1.4 2.1.5 2.1.6	Procedure Work Instructions	Government approved Contractor Format	10 days after government provides comments	N/A

PWS Objectives #	PWS Section	Deliverable Title	Format	Date of first submission	Subsequent Submission
2,3,4,5,6	1.4.5, 2.1.2.5, 2.1.1.9,	Functional Design Documents, Engineering Documents (DEVDOCS)	Government approved Contractor Format	10 days after government provides comments	N/A
2,3,5,6	1.4.5, 2.1.1.9, 2.1.2.3	Test Plan	Government approved Contractor Format	10 days after government provides comments	N/A
2,3,5,6	2.1.1.9, 2.1.2.3	Test cases	Government approved Contractor Format	10 days after government provides comments	N/A
2,3,5,6	2.1.1.9, 2.1.2.3	Test Scripts	Government approved Contractor Format	10 days after government provides comments	N/A
2,3,5,6	2.1.1.9, 2.1.2.3	Use Cases	Government approved Contractor Format	10 days after government provides comments	N/A
6	2.1.6.11	Draft Migration Plan	Government approved Contractor Format	90 days after award	N/A
6	2.1.6.11	Final Migration Plan	Government approved Contractor Format	10 days after Government provides comments	N/A
4	2.1.3.1 - 2.1.3.4	Draft training materials	Government approved Contractor Format	60 days after assessment	N/A

PWS Objectives #	PWS Section	Deliverable Title	Format	Date of first submission	Subsequent Submission
4	2.1.3.1 - 2.1.3.4	Final training materials	Government approved Contractor Format	10 days after Government provides comments	N/A